

PJ.17-01 SWIM-TI Purple Profile for A/G Advisory Information Sharing - Technical Specification TRL6

Deliverable ID:	**D2.2.615**
Dissemination Level:	**CO**
Project Acronym:	**PJ.17-01**
Grant:	**731826**
Call:	**H2020-SESAR-2015-2**
Topic:	**SESAR.IR-VLD.Wave1-20-2015**
Consortium Coordinator:	**THALES AIR SYS**
Edition Date:	**2 March 2020**
Edition:	**00.04.00**
Template Edition:	**02.00.02**

Founding Members

EUROPEAN UNION EUROCONTROL

SESAR JOINT UNDERTAKING

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
Antonio Strano / Leonardo	PJ.17-01 Solution leader	02/03/2020
Didier Lorido / THALES Avionics SAS	PJ.17-01 Member	12/12/2019
Jan Van Meenen / EUROCONTROL	PJ.17-01 Member	21/01/2019
Anna McLoughlin / AIRTEL	PJ.17-01 Member	21/01/2019
Norman Stewart / AIRTEL	PJ.17-01 Member	21/01/2019
Stéphane Abbas / AIRBUS	PJ.17-01 Member	21/01/2019
Dragos Borcea / SITA	PJ.17-01 Member	21/01/2019
Xavier Jourdain / THALES AIR SYS	PJ.17-01 Member	12/12/2019
José Ángel Álvarez Quirós / Indra	PJ.17-01 Member	12/12/2019
Jorge Morales Pérez / Indra	PJ.17-01 Member	24/02/2020
Frederic Antonio / AI DS CYBER	PJ.17-01 Member	12/12/2019

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
José Ángel Álvarez Quirós / Indra	PJ.17-01 Member	21/02/2020
Jan Van Meenen / EUROCONTROL	PJ.17-01 Member	27/02/2020
Jean-Pierre Becker / EUROCONTROL	PJ.17-01 Member	27/02/2020
Jesus Mario Garcia Cano / ENAIRE	PJ.17-01 Member	10/12/2019
Beatriz Sánchez López / ENAIRE	PJ.17-01 Member	10/12/2019
Stéphane Abbas / AIRBUS	PJ.17-01 Member	21/01/2019
Leonard Glaser-Opitz / LPS	PJ.17-01 Member	10/12/2019
Norman Stewart / AIRTEL	PJ.17-01 Member	21/01/2019
Anna McLoughlin / AIRTEL	PJ.17-01 Member	21/01/2019
Rowan Stewart / AIRTEL	PJ.17-01 Member	10/12/2019
Dragos Borcea / SITA	PJ.17-01 Member	21/01/2019
Armand Daraei / AI DS CYBER	PJ.17-01 Member	21/01/2019
Frederic Antonio / AI DS CYBER	PJ.17-01 Member	10/12/2019
Flavie Pontailler / Honeywell SAS	PJ.17-01 Member	10/12/2019
Xavier Jourdain / THALES AIR SYS	Project Coordinator	11/12/2019

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
Antonio Strano / Leonardo	PJ.17-01 Solution leader	28/02/2020
Leonard Glaser-Opitz / LPS	PJ.17-01 Member	28/02/2020
Didier Lorido / THALES Avionics SAS	PJ.17-01 Member	28/02/2020
Jean-Pierre Becker / EUROCONTROL	PJ.17-01 Member	28/02/2020
Rowan Stewart / AIRTEL	PJ.17-01 Member	02/03/2020
Stéphane Abbas / AIRBUS	PJ.17-01 Member	28/02/2020
Xavier Jourdain / THALES AIR SYS	Project Coordinator	28/02/2020
José Luis Santiago Navarro / Indra	PJ.17-01 Member	02/03/2020
Jesus Mario Garcia Cano / ENAIRE	PJ.17-01 Member	28/02/2020
Harald Milchrahm / FREQUENTIS	PJ.17-01 Member	28/02/2020
Flavie Pontailler / Honeywell SAS	PJ.17-01 Member	28/02/2020

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
00.00.01	16/07/2018	Draft	Antonio Strano	First revision of the TRL6 ToC based on feedback from TRL4 activities in terms of usability and accessibility.
00.00.02	03/08/2018	Revised draft	Antonio Strano	Updated §3 and §4 according to ECTL comments and planned updates.
00.00.03	03/09/2018	Revised draft	Antonio Strano	Updated §2.6, §3 and §4.
00.00.04	07/09/2018	Revised draft	Antonio Strano	Integrated and when applicable implemented comments from LPS, AIRTEL, TAV and AIRBUS. Implemented planned improvements.
00.00.05	11/10/2018	Revised draft	Antonio Strano	First version of the revised functional view starting from TRL4 TS and TRL6 messaging

Company General Use

				characterization.
00.00.06	09/11/2018	Revised draft	Antonio Strano	Updated §4.2 and added appendixes A, B and C.
00.00.07	21/11/2018	Revised draft	Antonio Strano, Didier Lorido, Anna McLoughlin	Updated §4.2.
00.00.08	04/12/2018	Revised draft	Antonio Strano, Didier Lorido	Updated §4.1, §4.2 and §B.2.
00.00.09	11/12/2018	Revised draft	Antonio Strano, Didier Lorido, Jan Van Meenen	Updated §3, §4.1 and §4.2.
00.00.10	21/12/2018	Revised draft	Antonio Strano, Didier Lorido, Anna McLoughlin	Updated §3, §4.1 and §4.2.
00.00.11	18/01/2019	Revised draft	Antonio Strano	Candidate final document content before importing requirements.
00.00.12	24/01/2019	Candidate final	Antonio Strano	Minor updates and requirements importing. Edition ready for the approvals.
00.01.00	28/01/2019	Final	Antonio Strano	Final edition for the handover.
00.01.01	03/04/2019	Revised draft	Antonio Strano	First edition of the final wave 1 TS based on D2.2.610 plus SJU assessment.
00.01.02	17/09/2019	Revised draft	Antonio Strano	Added initial comments and changes proposals from solution members review and prototyping activities.
00.01.03	04/11/2019	Revised draft	Antonio Strano	Added additional comments and changes proposals from solution members review and prototyping activities.
00.01.04	28/11/2019	Revised draft	Antonio Strano	Included the first draft of the Appendix F (SESAR and FAA Air-Ground SWIM comparison). Updated requirements status in accordance with TRL6 TVALR.

Company General Use

				Updated requirements REQ Trace in accordance to DS19. Implemented improvements from the TRL6 TVALR. Updated §4.1. in accordance with latest EATMA models. Added new security requirements recommended by AIRBUS Cyber Security.
00.01.05	09/12/2019	Revised draft	Antonio Strano	Implemented open points and received comments. Updated §4.1. Updated Subscription Management XSD. Updated references. Imported the spreadsheet with final set of requirements.
00.01.06	10/12/2019	Revised draft	Antonio Strano, Jorge Morales Pérez	Updated §4.1.
00.01.07	12/12/2019	Candidate final	Antonio Strano	Edition ready for the approvals.
00.02.00	16/12/2019	Final	Antonio Strano	Final edition for the handover.
00.02.01	21/01/2020	Revised draft	Antonio Strano	Implemented first set of comments following SJU assessment.
00.02.02	23/01/2020	Candidate final	Antonio Strano	Edition ready for the approvals.
00.03.00	27/01/2020	Final	Antonio Strano	Final edition for the handover.
00.03.01	20/02/2020	Revised draft	Antonio Strano	Updated following TRL6 maturity gate.
00.03.02	25/02/2020	Revised draft	Jorge Morales Pérez, Antonio Strano	Updated §4.1 according to the feedback from PJ.19. Implemented received comments on previous edition.
00.03.03	27/02/2020	Candidate final	Antonio Strano	Edition ready for the approvals.

Company General Use

00.04.00	02/03/2020	Final	Antonio Strano	Final edition for the handover.

Copyright Statement © –2020 – THALES AIR SYS, LPS SR (B4), EUROCONTROL, AIRTEL (NATMIG), INDRA, ENAIRE, LEONARDO, FREQUENTIS (FSP), Honeywell SAS, AIRBUS, THALES Avionics SAS, SITA, NAV PORTUGAL, LEONARDO GmbH, AI DS Cyber.

PJ.17-01

SWIM-TI PURPLE PROFILE FOR AIR/GROUND ADVISORY INFORMATION SHARING

This TS is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 731826 under European Union's Horizon 2020 research and innovation programme.



Abstract

The present document is the TRL6 Technical Specification (TS) concerning the technological solution PJ.17-01. Starting from the TRL4 [39] and then TRL6 [58] validation activities reports, the Purple Profile functional and technical architectures have been improved and functional and non-functional requirements updated accordingly.

Table of Contents

Abstract 7
1 Executive summary 15
2 Introduction 16
2.1 Purpose of the document 16
2.2 Scope 16
2.3 Intended readership 16
2.4 Background 16
2.5 Structure of the document 17
2.6 Glossary of terms 17
2.7 Acronyms and Terminology 34
3 SESAR Solution Impacts on Architecture 39
3.1 Target Solution Architecture 39
Purple Profile and Purple Profile enabled SWIM Services 41
OSED for aeronautical information (AIS) and meteorological (MET) data link services 45
3.2 Changes imposed by the SESAR Solution on the baseline Architecture 51
4 Technical Specifications 53
4.1 Functional architecture overview 56
4.2 Architectural Views 83
4.3 Functional and non-Functional Requirements 200
5 Implementation Options 590
6 Assumptions 591
7 References and Applicable Documents 592
7.1 Applicable Documents 592
7.2 Reference Documents 593
Appendix A Purple Profile SWIM Profile Assertion (SPA) 596
A.1 Scope 596
A.2 Rationale 597
A.3 Structure 599
A.3.1 Interoperability 599
A.3.2 Reuse and size 600
A.3.3 Constraints, competing requirements and risks 600
A.3.4 Modular structure 600
A.3.5 Lifecycle of the SWIM Profile 600

Company General Use

A.3.6 Design rules 601
A.3.7 Design criteria 601
A.3.8 Recommended structure 601

A.4 Conformance Statements 604

Appendix B MEPs and Messaging characterization 606

B.1 FDRMR-MEP definition 606
B.1.1 Fully decoupled Request/Multi-Response MEP 608

B.2 Messaging characterization 608
B.2.1 Statement of applicability to Purple Profile 609

Appendix C PJ.17-01 requirements guidance 636

C.1 Specific template for requirement text 636
C.1.1 Interface Bindings 636
C.1.2 Measurements 637

C.2 SWIM-TI specific requirement attributes 638
C.2.1 “Profile Part" Attribute 638
C.2.2 “Domain of interest" Attribute 639
C.2.3 "Point of view" Attribute 641
C.2.4 "Role" Attribute 641
C.2.5 “Selfstanding set" Attribute 642
C.2.6 “Testability" Attribute 644

C.3 SWIM-TI specific requirement links 644
C.3.1 <ATMS Requirement> Linked Element Type 644

Appendix D Subscription Management XML schema 646

Appendix E MS Excel export of PJ.17-01 requirements 647

Appendix F SESAR and FAA Air-Ground SWIM comparison 648

F.1 Operational perspective 648

F.2 Technical perspective 649

F.3 Deployment perspective 653

Appendix G PJ.17-01 requirements to be addressed in future activities 654

List of Tables

Table 1: Glossary 34

Table 2: Acronyms and terminology 38

Table 3: SESAR Solution PJ.17-01 Scope and related Functional Blocks/roles & Enablers 40

Table 4: SWIM Purple Profile technical use cases 44

Table 5: ED-151 Data link modes 46

Table 6: ED-151 Data link modes and SWIM-TI MEPs/MEP families 47

Table 7: List of Capability Configuration required for the SESAR Solution 51

Table 8: List of changes due to the SESAR Solution 52

Table 9: Bindings (Use) Elements with related service interfaces (use elements) and system ports... 82

Table 10: List of Concerns framed by the functional viewpoint 84

Table 11: List of Actors interested to the functional viewpoint..... 84

Table 12: List of Concerns framed by the technical viewpoint 85

Table 13: List of Actors interested to the technical viewpoint 85

Table 14: List of Concerns framed by the deployment viewpoint 86

Table 15: List of Actors interested to the deployment viewpoint 86

Table 16: SWIM Purple Profile technical use cases and non-functional characteristics..... 88

Table 17: Messaging functions applicability to Purple Profile 92

Table 18: Security functions applicability to Purple Profile 94

Table 19: Purple Profile Lifespan/Lifetime QoS 96

Table 20: Purple Profile Ordering guarantees QoS 98

Table 21: Purple Profile durability QoS 101

Table 22: Purple Profile Delivery guarantees QoS 104

Table 23: Security functions and SESAR2020 SCs..... 108

Table 24: SWIM Purple Profile technical use cases and information distribution mechanisms..... 122

Table 25: Purple Profile Subscription Request Message..... 134

Table 26: Purple Profile Subscription Request Message - Filter type 135

Table 27: Purple Profile Fixed termination time subscription policy 135

Table 28: Purple Profile Subscription Response Message 135

Table 29: Purple Profile Subscription Response Message - SubscriptionReferenceType..... 136

Table 30: Purple Profile Subscription Response Message – SubscriptionFault enumeration 136

Table 31: Purple Profile Unsubscription Request Message 137

Table 32: Purple Profile Unsubscription Response Message 137

Table 33: Purple Profile Unsubscription Response Message – UnsubscriptionFault enumeration.... 137

Table 34: Purple Profile Active Subscriptions Request Message 138

Table 35: Purple Profile Active Subscriptions Response Message 139

Table 36: Purple Profile Active Subscriptions Response Message - SubscriptionType 139

Table 37: Purple Profile Active Subscriptions Response Message – ActiveSubscriptionsProcessingFault enumeration 139

Table 38: Purple Profile Subscription Renew Request Message 140

Table 39: Purple Profile Subscription Renew Response Message 140

Table 40: Purple Profile Subscription Renew Response Message – SubscriptionRenewFault enumeration 140

Table 41: Purple Profile UpdateSubscriptionFilter Request Message 141

Table 42: Purple Profile UpdateSubscriptionFilter Response Message 141

Table 43: Purple Profile UpdateSubscriptionFilter Response Message – UpdateSubscriptionFilterFault enumeration 142

Table 44: Purple Profile ActiveSubscriptionsNotify Message 142

Table 45: Messaging entities instantiation over AMQP 1.0 145

Table 46: Purple Profile Lifespan/Lifetime QoS instantiation over AMQP 1.0 149

Table 47: Purple Profile durability QoS instantiation over AMQP 1.0 151

Table 48: Purple Profile Delivery guarantees QoS instantiation over AMQP 1.0 154

Table 49: Non-nominal events and delivery guarantees 155

Table 50: Reconnection and retry policy 157

Table 51: Purple Profile Ordering guarantees QoS instantiation over AMQP 1.0 159

Table 52: AMQP content-type and content-encoding for application level compression 160

Table 53: AMQP message annotation for on-the-fly compression 160

Table 54: Security functional view to technical view 164

Table 55: Purple Profile message level security information distribution 167

Table 56: OCSP and CRL related non-nominal cases 168

Table 57: Fully decoupled Request/Response over AMQP binding 175

Table 58: Request/Response over AMQP federation binding 176

Table 59: Publish/Subscribe over AMQP binding 179

Table 60: Publish/Subscribe over AMQP federation binding 181

Table 61: AMQP 1.0 annotated message Header section 181

Table 62: AMQP 1.0 annotated message delivery and message annotation sections 181

Table 63: AMQP 1.0 annotated message properties and application-properties sections 183

Table 64: AMQP 1.0 annotated message restrictions for message level security 184

Table 65: AMQP 1.0 annotated message footer restrictions 185

Table 66: AMQP 1.0 subject properties field values for subscription management messages 186

Table 67: Minim set of avionics parameters used by the Air SWIM Node 187

Table 68: Technical-Functional views traceability 190

Table 69: Impacts of EFBPU installation choices 193

Table 70: Impacts of NSU installation choice 194

Table 71: Impacts of mix EFBPU & NSU installation choice 196

Table 72: Air PP SWIM Node installation main impacts on aircraft airworthiness and operators' processes 197

Table 73: Consolidate load characterization for time behaviour requirements 410

Table 74: Security functions and ISO/IEC 25010:2011 security sub-characteristic 420

Table 75: PJ.17-01 TRL4 TS assumptions 591

Table 76: Purple Profile scope and key elements 596

Table 77: Extended MEP characterization 607

Table 78: per-entity SoA – applicability 613

Table 79: per-entity SoA - mandatoriness 614

Table 80: per-event SoA – applicability 618

Table 81: per-event SoA - mandatoriness 622

Table 82: per-characteristic SoA - applicability 628

Table 83: per-characteristic SoA - mandatoriness 635

Table 84: SWIM-TI <ATMS Requirement> Linked Element Type relationships 645

Table 85: In progress requirements 667

List of Figures

Figure 1: SWIM Purple Profile and SWIM Services (conceptual) 45

Figure 2: What, How and How good aspects relationships 54

Figure 3: Artifact Structure Diagram - SWIM Purple Profile Ground 57

Figure 4: Artifact Assembly Diagram - SWIM Purple Profile Ground 57

Figure 5: Artifact Structure Diagram - SWIM Purple Profile Air 58

Figure 6: Artifact Assembly Diagram - SWIM Purple Profile Air 58

Figure 7: NSV-1 [Context] Exchange of MET Information through Purple Profile 59

Figure 8: NSV-1 [Context] Exchange of AIS Information through Purple Profile 60

Figure 9: [NSV-4] Uplink MET over PS-MEP- Subscription Management 62

Figure 10: [NSV-4] Uplink MET over PS-MEP – Publication Message Distribution 63

Figure 11: [NSV4] Downlink MET over PS-MEP – Subscription Management 65

Figure 12: [NSV4] Downlink MET over PS-MEP – Publication Message Distribution 66

Figure 13: [NSV4] Uplink MET over FDRR-MEP 68

Figure 14: [NSV4] Uplink MET over FDRR-MEP – Aircraft and Ground Purple Profile enabled applications authentication and authorization 70

Figure 15: [NSV4] Uplink MET over FDRR-MEP – Air SWIM Node authentication and authorization .. 71

Figure 16: MET NSV-2 Infrastructure Connectivity Model 73

Figure 17: AIS NSV-2 Infrastructure Connectivity Model 74

Figure 18: Infrastructure connectivity model within the Civil Aircraft CC 75

Figure 19: Infrastructure connectivity model within the ATM-MET CC 75

Figure 20: Infrastructure connectivity model within the SWIM Identity Management CC 76

Figure 21: Infrastructure connectivity model within the Regional AIM CC 76

Figure 22: Infrastructure connectivity model within the Aerodrome ATM-MET CC 77

Figure 23: Infrastructure connectivity model within the TWR CC 78

Figure 24: Resource Architecture Structure Diagram within the Civil Aircraft CC 79

Figure 25: Artifact Assembly Diagram within the Aircraft Technical System 80

Figure 26: Artifact Assembly Diagram within the 4DWxCube Technical System 81

Figure 27: SWIM-TI Security functional view 105

Figure 28: Purple Profile layered functional view 109

Figure 29: Purple Profile layered functional view interfacing layers 111

Figure 30: ARINC Report 821 Aircraft Network Services 118

Figure 31: Purple Profile technical view – cardinality of the relationships between main entities 122

Figure 32: PPUC-01 and PPUC-03 (Request/Response) conceptual view 124

Figure 33: Purple Profile PPUC-01 technical view 126

Figure 34: Purple Profile PPUC-03 technical view 128

Figure 35: Purple Profile PPUC-02 technical view 130

Figure 36: Purple Profile PPUC-04 technical view 132

Figure 37: AMQP 1.0 based Message Queue(MQ) 146

Figure 38: AMQP 1.0 based Message Topic(MT) and Subscription handler 147

Figure 39: AMQP Connections and entities initiating the connection 156

Figure 40: Communications Network Infrastructure 170

Figure 41: EFBPU installation and cockpit side synchronisation option 1 192

Figure 42: EFBPU installation and cockpit side synchronisation option 2 193

Figure 43: NSU installation 194

Figure 44: Mix Installation of EFBPU & NSU 195

Figure 45: Purple Profile Profile Parts design 602

Figure 46: ED-151 Contract datalink mode end to end behaviour 606

Figure 47: FDRMR-MEP Sequence diagram 608

1 Executive summary

The present document is the TRL6 Technical Specification (TS) concerning the technological solution PJ.17-01. Starting from the TRL4 results [39], the Purple Profile functional and technical architectures have been improved and functional and non-functional requirements updated accordingly.

Main improvements with respect to TRL4 include:

- Architecture description based on viewpoints (functional, technical and deployment).
- Avionics architectural considerations and installation option analysis.
- Analysis of major non-nominal cases.
- Safety requirements.
- Security requirements improvement.
- Reliability requirements.
- Performance requirements.
- Interface requirements

The above have been identified and implemented taking into account analysis and recommendations from TRL4 TVALR [39]. Furthermore, EATMA NAF diagrams included in this edition are being updated taking into account PJ.19-03 feedback assessed during PJ.17-01 TRL4 maturity gate.

Finally, also the recommendations from the TRL6 TVALR [58] applicable to the TS have been taken into account, assessed and the TS updated accordingly. The requirements status has been updated taking into account requirements coverage from the TRL6 TVALR [58]. Requirements still “in progress” (i.e. not validated) are reported in the Appendix G.

2 Introduction

The present document is the TRL6 Technical Specification (TS) concerning the technological solution PJ.17-01. Starting from the analysis and recommendations from TRL4 TVALR [39], following main improvements with respect to TRL4 have been provided as part of this TS:

- Architecture description based on viewpoints (functional, technical and deployment).
- Avionics architectural considerations and installation option analysis.
- Analysis of major non-nominal cases.
- Safety requirements.
- Security requirements improvement.
- Reliability requirements.
- Performance requirements.
- Interface requirements.

2.1 Purpose of the document

This document provides architectural viewpoints description and requirements specification covering functional, non-functional and interface requirements concerning the Purple Profile technical systems (Ground Purple Profile and Air Purple Profile).

2.2 Scope

The aim of this Technical Specification (TS) is to provide functional, non-functional and interface requirements for technological solution PJ.17-01 for TRL6. Requirements included in this specification will be validated (technical validation) by the PJ17-01 validation exercises planned for TRL6.

This TS will be further refined, before finalizing SESAR2020 wave1, taking into account TRL6 validation activities.

2.3 Intended readership

The intended readership of the present document is as follows:

- SJU to assess and to manage this SESAR 2020 deliverable.
- PJ.19 to assess this deliverable in accordance with its role.
- Any SESAR 2020 projects and solutions interested in the PJ.17-01 TRL6 technical specification (e.g. PJ.14-02.04, PJ18-04a/b/c).

2.4 Background

This TS is built on the harmonization and improvement of the TRL4 TS [38] as recommended in the TRL4 TVALR [39] and briefly summarized in the introduction of this chapter.

2.5 Structure of the document

This document is organized as follows:

- §1 executive summary.
- §2 Introduction: general introduction, scope and purpose of the document. This chapter provides also the glossary of terms, acronyms and terminology used in this TS.
- §3 Solution Impacts on Architecture: overview of the architecture and relationships with EATMA.
- §4 Technical Specifications: architecture viewpoint introduction, definition and requirements.
- §5 Implementation options: descriptions of the implementation options identified in this TS.
- §6 Assumptions.
- §7 References and applicable documents.
- Appendix A: Purple Profile SWIM Profile Assertion SPA.
- Appendix B: MEPs and messaging characterization.
- Appendix C: PJ.17-01 specific requirements guidance.
- Appendix D: Purple Profile Subscription Management messages XML schema.
- Appendix E: MS Excel export of PJ.17-01 requirements included in this TS.
- Appendix F: high level comparison of SESAR and FAA Air-Ground SWIM.
- Appendix G: PJ.17-01 requirements to be addressed in future activities.

2.6 Glossary of terms

Term	Definition	Source of the definition
Access Control	ITU-T IdM X.1252 defines this term as a procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party	ITU-T IdM X.1252
A/G SWIM Access Point	Either Aircraft A/G SWIM Access Point or Ground A/G SWIM Access Point	PJ.17-01
Address	ITU-T IdM X.1252 defines this term as an identifier for a specific termination point that is used for routing	ITU-T IdM X.1252
Advisory Purple Profile Enabled	Purple Profile Enabled SWIM Service concerning	PJ.17-01

Company General Use

SWIM Service	Air/Ground advisory information sharing.	
Agent	ITU-T IdM X.1252 defines this term as an entity that acts on behalf of another entity.	ITU-T IdM X.1252
Air/Ground advisory information sharing	Sharing of supplemental information that is not necessary for and not directly interfering with the command and control of an aircraft. The intended use is to provide flight crews with information improving common situational awareness and enabling collaborative decision making process.	PJ.17
Air/Ground safety-critical information sharing	Sharing of information that supports safety of life and has an impact on tactical command and control of an aircraft. Information exchanges concerning strategic decisions are not considered having safety effects.	PJ.17
Aircraft Meteorological Data Relay	WMO (World Meteorological Organization) program for reporting and collecting automatic meteorological reports from aircraft.	Eurocae ED-151
Air A/G SWIM Access Point	See Air Purple Profile SWIM Node.	PJ.17-01
Air Purple Profile SWIM Node	SWIM Node specialization providing aircraft side capabilities of the Air-Ground SWIM segment.	PJ.17-01
Air–Ground SWIM segment	A set of Aircraft and Ground capabilities that allow Aircraft SWIM Enabled applications to interact with Ground SWIM Enabled applications via provisioning and consumption of SWIM Services. The SWIM Purple profile is covering the needs and constraints identified for this segment.	PJ.17-01
Alarm	An indication of an error or an abnormal and/or undesirable condition for a resource. An example of an alarm would be for a “connection down” in a data communications channel, or a non-booting processor in a hardware platform. Alarms originate with the hardware, software, and data communications infrastructure, and the infrastructure provides an indication to the Supervision when an alarm is raised or cleared. The Supervision notifies the local owner or authorized requester when an alarm is raised or cleared for a monitored resource.	SESAR1 WP14
Alliance	ITU-T IdM X.1252 defines this term as an agreement between two or more independent entities that defines how they relate to each other and how they	ITU-T IdM X.1252

	jointly conduct activities.	
Archive	Information storage that is used for by the automation for long-term retention of information produced and/or used at the local SWIM Node. An archive may be offline with respect to the SWIM Node, meaning that it is not directly accessible to processes and services running on the SWIM Node; or it may be online with respect to the SWIM Node, meaning that the archive is directly accessible to processes and services running on the SWIM Node. Information that is logged by the SWIM Supervision is retained online for a configurable time period, after which it is archived and is then no longer guaranteed to be available in the same manner as information that has not reached its retention time limit. Each SWIM Node will have local processes and procedures for storing, maintaining, and accessing archived information. Archived information will be available to the reporting capability; however, the response time for accessing archived information will vary according to the storage approach used by the node.	SESAR1 WP14
Assertion	ITU-T IdM X.1252 defines this term as a statement made by an entity without accompanying evidence of its validity.	ITU-T IdM X.1252
ATM Service or SWIM ATM Service	A service representing the exchange of well-defined ATM information.	SESAR1 WP14
Attribute	ITU-T IdM X.1252 defines this term as information bound to an entity that specifies a characteristic of the entity.	ITU-T IdM X.1252
Attribute Based Access Control (ABAC)	In attribute-based access control (ABAC), access is based on attributes of the user. The user has to prove these attributes to the access control engine. An attribute-based access control policy specifies which attributes need to be satisfied in order to grant access to an object.	SESAR1 WP14
Attribute Value	ITU-T IdM X.1252 defines this term as a particular instance of the class of information indicated by an attribute type.	ITU-T IdM X.1252
Authentication (Entity)	ITU-T IdM X.1252 defines this term as a process used to achieve sufficient confidence in the binding between the entity and the presented identity.	ITU-T IdM X.1252

Company General Use

Authorization	ITU-T IdM X.1252 defines this term as the granting of rights and, based on these rights, the granting of access.	ITU-T IdM X.1252
Authorized requester	A human user or automated process, at the local SWIM Node or at a remote SWIM Node, that has been authenticated and is authorized per security requirements to make a service request.	SESAR1 WP14
Binding	ITU-T IdM X.1252 defines this term as an explicit established association, bonding, or tie.	ITU-T IdM X.1252
Bridge Certificate Authority (BCA)	The Bridge Certification Authority (BCA) architecture addresses the shortcomings of the two basic PKI architectures, and to link PKIs that implement different architectures. The BCA does not issue certificates directly to users. The BCA is not intended to be used as a trust point by the users of the PKI, unlike the "root" CA in a hierarchy. The BCA establishes peer-to-peer trust relationships with the different user communities, which allows the users to keep their natural trust points. These relationships are combined to form a "bridge of trust" enabling users from the different user communities to interact with each other through the BCA with a specified level of trust.	SESAR1 WP14
Certificate	ITU-T IdM X.1252 defines this term as a set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data.	ITU-T IdM X.1252
Certificate Service Provider (CSP)	It is anticipated that security of the European SWIM-TI neither be handled by a single certification authority nor even by a single hierarchy of certification authorities. The main reason is that a few organizations (e.g. CFMU and some Airlines) have already deployed a PKI with an associated third party CA (or Certificate Service Provider (CSP)). The objective is not to replace the existing CAs by a single new one but rather to build a SWIM-TI capable of federating existing CAs and the SWIM-TI dedicated CA	SESAR1 WP14
Channel Protection	Channel Protection or transport level security, provides point-to-point protection of the communication. The protection will not go beyond intermediaries. This may be acceptable or not depending on the context. The Transport Layer Security TLS (cryptographic protocol) is a well-known	SESAR1 WP14

	and widely used protocol to provide transport level security. TLS encrypts the data using asymmetric cryptography for key exchange, symmetric encryption for confidentiality and Message Authentication Codes for message integrity.	
Claim	ITU-T IdM X.1252 defines this term as to state as being the case, without being able to give proof.	ITU-T IdM X.1252
Confidentiality Ensuring	Confidentiality Ensuring aims at providing the ability to ensure "non-disclosure" of information. This service relies on the policy enforcement features and to the cryptographic mechanisms provided by the Cryptography security enabler to ensure information confidentiality at message level.	SESAR1 WP14
Credential	ITU-T IdM X.1252 defines this term as a set of data presented as evidence of a claimed identity and/or entitlements.	ITU-T IdM X.1252
Data Element	A formalised representation of data. Data Elements are exchanged by Technical Systems when invoking operations in Service Interfaces or System Ports.	EATMA
Data Origin Authentication	Equivalent expression for Information Origin Authentication	SESAR1 WP14
Data Validation	Data validation allows checking for conformance to message/data type descriptions. The conformance conditions are expressed in form of well-defined policy assertions assigned to the SWIM service definition.	SESAR1 WP14
Dead letter queue	In message queuing, the dead letter queue stores messages that cannot or should not be delivered. Examples of criteria for moving messages to a dead letter queue are: message is sent to a queue that does not exist; queue length limit is exceeded; message length limit is exceed; invalid message; unreachable destination.	PJ.17-01
Delegation	ITU-T IdM X.1252 defines this term as an action that assigns authority, responsibility, or a function to another entity.	ITU-T IdM X.1252
Digital Identity	ITU-T IdM X.1252 defines this term as a digital representation of the information known about a specific individual, group or organization.	ITU-T IdM X.1252

Company General Use

Digital Signature (algorithm)	Digital Signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that a known sender created the message, and that it was not altered in transit. Unlike a Message Authentication Code, a Digital Signature also provides support for non-repudiation.	SESAR1 WP14
Electronic Flight Bag	An information system for flight deck crew members which allows storing, updating, delivering, displaying, and/or computing digital data to support flight operations or duties.	EASA AMC 20-25/ FAA AC-120
EFB software application	Software installed on an EFB system that allows specific operational functionality.	EASA AMC 20-25/ FAA AC-120
EFB system	An EFB system comprises the hardware (including any battery, connectivity provision, I/O devices) and software (including databases) needed to support the intended EFB function(s).	EASA AMC 20-25/ FAA AC-120
Enabling Service	A service provided by the SWIM-TI.	SESAR1 B4.3/WP14
Entity	ITU-T IdM X.1252 defines this term as something that has separate and distinct existence and that can be identified in context. An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.	ITU-T IdM X.1252
European Network of Excellence in Cryptology (ECRYPT)	ECRYPT (European Network of Excellence for Cryptology) is a 4-year European research initiative launched on 1 February 2004. The stated objective is to, "intensify the collaboration of European researchers in information security and more in particular in cryptology and digital watermarking".	ECRYPT
Failure Transparency	Failure transparency masks from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. When this transparency is provided, the designer can work in an idealized world in which the corresponding class of failures does not occur.	SESAR1 WP14
Federation	In the security context, ITU-T IdM X.1252 defines this term as an association of users, service providers, and	ITU-T IdM X.1252

Company General Use

	identity service providers. Guidance: This term is not to be confused with similar term used in the context of messaging federation.	
Functional Status	Indicates the ability of the SWIM Node or an element of the SWIM Node to provide the services.	SESAR1 WP14
Ground A/G SWIM Access Point	See Ground Purple Profile SWIM Node.	PJ.17-01
Ground Purple Profile SWIM Node	SWIM Node specialization providing ground side capabilities of the Air-Ground SWIM segment.	PJ.17-01
Ground-Ground SWIM segment	A set of Ground capabilities that allow Ground SWIM Enabled applications to interact via SWIM Services. This SWIM segment has been further segmented identifying the SWIM Yellow and Blue profiles	PJ.17-01
Identification	ITU-T IdM X.1252 defines this term as the process of recognizing an entity by contextual characteristics.	ITU-T IdM X.1252
Identifier	ITU-T IdM X.1252 defines this term as one or more attributes used to identify an entity within a context.	ITU-T IdM X.1252
Identity	ITU-T IdM X.1252 defines this term as a representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.	ITU-T IdM X.1252
Identity Management (IdM)	ITU-T IdM X.1252 defines this term as a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions)	ITU-T IdM X.1252

Company General Use

	used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications.	
Identity Provider (IdP)	ITU-T IdM X.1252 defines this term as an entity that verifies, maintains, manages, and may create and assign identity information of other entities. Depending on the type of digital identity, an Identity Provider may be Public Key Infrastructure (PKI) or Security Token Infrastructure (STI). IdP is also named Identity Service Provider (IdSP).	ITU-T IdM X.1252
Information Origin Authentication	SWIM-TI service to ensure integrity of the message and to authenticate its originator by several techniques at message level and transport level. Information Origin Authentication is synonymous with Data Origin Authentication are.	SESAR1 WP14
Installed EFB	An EFB host platform installed in the aircraft and considered as an aircraft part, covered, thus, by the aircraft airworthiness approval.	EASA AMC 20-25/ FAA AC-120
Interface binding	See SWIM Interface binding.	SESAR1 WP14
Interface Control Document (ICD)	An interface control document (ICD) in systems engineering and software engineering, describes the interface or interfaces between subsystems or to a system or subsystem.	SESAR1 WP14
Message Queue	Point-to-point distribution mechanism. Messages can be sent to a particular Message Queue designated to hold messages for a specific application. The Message Queue will hold the message until it is extracted by this application. Note that the term Message Queue is technology agnostic. It should not be confused with similar features of some technical systems	PJ.17-01
Message Queue	The Message Queue represents technology/messaging protocol agnostic messaging capability providing the Message Queue distribution mechanism.	PJ.17-01
Message Topic	Message Topic: Distribution mechanism for publishing messages that are delivered to multiple subscribers. Applications are publishing messages to a particular message topic designated to hold messages for subscribed applications. Applications may register interest in receiving messages (subscribe) on a	PJ.17-01

	particular message topic. The Message Topic then routes messages from the publishing applications to subscribed applications. Note that the term Message Topic is technology agnostic. It should not be confused with similar features of some technical systems	
Message Topic	The Message Topic represents technology/messaging protocol agnostic messaging capability providing the Message Topic distribution mechanism.	PJ.17-01
Messaging FB or SWIM-TI Messaging FB	Messaging Functional Block provides varying degrees of decoupled, interoperable and effective communications between information producer and information consumers. It supports different message exchange patterns (e.g. publish/subscribe, request/response, push, etc.), different subscription styles (e.g. durable, non-durable) and different set of QoS (e.g. best-effort and reliable delivery).	SESAR1 WP14
Mutual Authentication	ITU-T IdM X.1252 defines this term as a process by which two entities (e.g., a client and a server) authenticate each other such that each is assured of the other's identity.	ITU-T IdM X.1252
Non-Repudiation	ITU-T IdM X.1252 defines this term as the ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.	ITU-T IdM X.1252
Pan-European Network Service (PENS)	A joint EUROCONTROL-ANSPs led initiative to provide a common IP based network service across the European region covering voice and data communication and providing efficient support to existing services and new requirements that are emerging from future Air Traffic Management (ATM) concepts.	SESAR
Persistent	ITU-T IdM X.1252 defines this term as existing and able to be used in services outside the direct control of the issuing assigner, without a stated time-limit.	ITU-T IdM X.1252
Policy (Security)	An agreement upon which entities (e.g. Systems) can collaborate. A typical example of this is Authorization Policy and Audit Policy.	SESAR1 WP14
Policy Life Cycle Management (Security)	The Policies lifecycle management is a key concept enabling (security) policies management and proper (security) policies enforcement.	SESAR1 WP14

Company General Use

Portable EFB	A portable EFB is a portable EFB host platform, used on the flight deck, which is not part of the certified aircraft configuration.	EASA AMC 20-25/ FAA AC-120
Public Key Cryptography	Public Key Cryptography refers to a cryptographic technique in which one key is secret private and a corresponding key one is public. Information are is encrypted using the public key and can only be decrypted by the corresponding secret/private key or vice-versa, information is encrypted using the private key and can only be decrypted by the corresponding public key. Public Key Cryptography can also be used for Digital Signatures; in this case the private key is used for signing, and the corresponding public key for verifying.	SESAR1 WP14
Public Key Infrastructure	A Public Key Infrastructure (PKI) is a system, which may include hardware, software, human in the loop, policies and procedures, needed to create, manage, distribute, use, store and revoke digital identities in X.509 certificates based IdM. PKIs represent the instantiation of the ITU-T X.1252 IdP when the X.509 certificates based security is adopted.	SESAR1 WP14
Purple Profile aircraft and ground asynchronous messaging capabilities federation	Architecture, requirements and configurations describing the federation of the messaging capabilities between Air Purple Profile SWIM Node and Ground Purple Profile SWIM Node.	PJ.17-01
Purple Profile technical architecture	The Technical View of the Purple Profile. Guidance (PJ.17-01): The SWIM-TI TAD defines 3 views: functional, technical and deployment.	PJ.17-01
Purple Profile SWIM Node	Either Air Purple Profile SWIM Node or Ground Purple Profile SWIM Node	PJ.17-01
Purple Profile Enabled SWIM Service	SWIM Service consumed or provided over the Purple Profile. Guidance (PJ.17-01): The design artefacts characterizing a SWIM Service over the Purple Profile are: - Pair of aircraft and ground «Service Binding» used to consume/provide the service.	PJ.17-01

Company General Use

	- Service specific artefacts describing the «contract» field of the selected «Service Binding» pair. - Purple Profile Messaging Technical architecture and related configuration aspects. Purple Profile Enabled SWIM Services are further characterized as: - Advisory Purple Profile Enabled SWIM Service, - Safety-critical Purple Profile Enabled SWIM Service.	
Recording Functional Block or SWIM-TI Recording FB	Recording FB includes the ability to collect, store and to retrieve on demand of information related to communication being performed via the SWIM Interfaces and supervision actions and events.	SESAR1 WP14
Registry Functional Block or SWIM-TI Registry FB	Registry FB includes two main groups of functions: - Information Management enabling the management several kinds of ATM-specific service meta-data allowing to discover, to subscribe and to publish/update these information. - Policy Management enabling the definition, validation and distribution of several kinds of policies including security. It covers policy administration (including creation, maintenance, change and deletion) and policy distribution and transformation and policy auditing.	SESAR1 WP14
Replication Transparency	Replication transparency masks the use of a group of mutually behaviourally compatible objects to support an interface. Replication is often used to enhance performance and availability.	SESAR1 WP14
Revocation	ITU-T IdM X.1252 defines this term as the annulment by someone having the authority, of something previously done.	ITU-T IdM X.1252
SAML Token	Security Assertion Markup Language (Token)	SAML
Safety-critical Purple Profile Enabled SWIM Service	Purple Profile Enabled SWIM Service concerning Air/Ground information sharing having safety effects.	PJ.17-01
Schematron	In markup languages, Schematron is a rule-based validation language for making assertions about the presence or absence of patterns in XML trees. It is a structural schema language expressed in XML using a	SESAR1 WP14

	small number of elements and XPath.	
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.	ITU-T IdM X.1252
Security Domain	ITU-T IdM X.1252 defines this term as a set of elements, a security policy, a security authority, and a set of security-relevant activities in which the elements are managed in accordance with the security policy.	ITU-T IdM X.1252
Security Functional Block or SWIM-TI Security FB	Security Functional Block provides confidentiality, integrity, access control, accountability and non-repudiation functionalities, allowing data exchanged through the SWIM-TI to be protected	SESAR1 WP14
Security Risk Assessment	The overall process of risk identification and risk evaluation.	16.06.02 D103 SESAR Security Ref Material Level
Security Token	Security tokens are used to prove one's identity electronically. The token acts like an electronic key to access something. Besides the information needed to authenticate an identity, a token can provide additional information (identity attributes) that are used for (e.g.) authorization purposes. Security tokens imply trust of a third party that issues the security tokens.	SESAR1 WP14
Security Token Infrastructure (STI)	A Security Tokens Infrastructure (STI) is a system, which may include hardware, software, human in the loop, policies and procedures, needed to create, manage, distribute, use, store and revoke digital identities in security token based IdM. STIs represent the instantiation of the ITU-T X.1252 IdP when the security tokens based security is adopted.	SESAR1 WP14
Security Token Service (STS)	A Security Token Service (STS) is a software based identity provider responsible for issuing and verifying security tokens as part of a claims-based identity management.	SESAR1 WP14
Service	The contractual provision of something (a non-physical object), by one, for the use of one or more others.	EATMA

Company General Use

	Services involve interactions between providers and consumers, which may be performed in a digital form (data exchanges) or through voice communication or written processes and procedures. Guidance: Services are key to describe the relationships between the different aspects of the Architecture: operational and solution. Services have one or more Service Interfaces.	
Service Agent SOA Design Pattern	Service agents can be designed to automatically respond to predefined conditions without invocation via a published contract. Refer to SOA Patterns http://www.soapatterns.org/service_agent.php	SOA Patterns
Service instance	The actual implementation of applicable Service Interfaces Definitions by a stakeholder.	SWIM Foundation/Compliance
Service Interface	The mechanism by which a service communicates. Guidance: The Service Interface is the actual endpoint (port) by which the Service communicates.	EATMA
Service Interface Definition	The specification of the service interface.	EATMA
Service Virtualization (Through Service Agent SOA design pattern)	Service Virtualization helps insulate service infrastructure details such as service endpoint location, service inter-connectivity, policy enforcement, service versioning and dynamic service management information from service consumers. Refer to: http://www.soapatterns.org/service_virtualization.php	SOA Patterns
Shared Object Functional Block or SWIM-TI Shared Object FB	Shared Object FB is a special category that holds a pattern used to share data across multiple SWIM Nodes according to specific roles and rules.	SESAR1 WP14
Supervision Functional Block or SWIM-TI Supervision FB	Monitoring and Control FB includes control, fault management and performance monitoring at SWIM Node level (local supervision).	SESAR1 WP14
SWIM Access Point	A SWIM access point is a logical entity which bundles a number of technical capabilities (e.g. messaging, security, logging, interface management, etc.). Guidance (PJ.17-01): ICAO SWIM Access Point and SWIM Node are	ICAO Doc 10039, Manual on SWIM Concept. (draft edition available

Company General Use

	understood as to be conceptually the same.	at March 2017)
SWIM Enabled application	(1) A SWIM Enabled System/Application is a system/application exchanging information with other ATM actors according to the SWIM ATM Services and the appropriate SWIM-TI. (2) A SWIM enabled application consumes or provides SWIM information services using SWIM standards. Also referred to as "application". Guidance (PJ.17-01): Service Provider and Consumer roles are in general applicable to organizations, people and applications/systems. In EATMA services are consumed or provided by Capability Configurations or Technical Systems and Service Instances are consumed or provided by "Instances of" Capability Configurations or Technical Systems. In the SWIM Purple Profile specification (technical view) the Service Provider and Consumer roles are intended to be played by SWIM enabled applications which: - Represent instances of EATMA Technical Systems belonging to specific Capability Configuration that - Consume or provide SWIM services using SWIM standards.	(1) SESAR 1 SWIM-TI TAD/TSs (2) ICAO Doc 10039, Manual on SWIM Concept (draft edition available at March 2017).
SWIM Enabled system	See SWIM Enabled application	SESAR 1 P14.01.03 D30
SWIM Interface binding	Standard based protocol stack (technical interoperability). In the context of SWIM-TI, following interface binding types are defined: - <Service binding>. This kind of binding is external to the SWIM-TI and related to SWIM service only. - <Internal service binding>. This kind of binding is internal to the SWIM-TI only and related to internal service (e.g. PKI services). - <Network binding>. This kind of binding is external to the SWIM-TI and related to the Network only. - <External service binding>. This kind of binding is external to the SWIM-TI and not a <Service binding> or a <Network binding> (e.g. Time Service).	SESAR 1 P14.01.03 D30
SWIM Message Exchange	A Message Exchange Pattern (MEP) or interaction pattern describes how different parts of a message passing system connect and communicate with each	SESAR 1 P14.01.03 D39 and P14.01.03 D30

Company General Use

Pattern (MEP)	other. A MEP describes the roles of distinct participants, their individual actions, and the sequence of messages in a distributed collaborative action in order to achieve an objective in a predictable manner. In order to ensure interoperability, all participants need to share the same understanding of the MEP and act as prescribed by the MEP. MEPs can exist at various levels of abstraction and any MEP can be emulated on top of another MEP. MEPs are characterised through four groups of attributes: Conversation direction, Cardinality, Decoupling (Time, Space and Synchronization) and Push/Pull.	
SWIM Node or SWIM-TI Node	A SWIM-TI Node is an autonomous point of presence in the Distributed System (of Systems) that interacts with other SWIM-TI Nodes in the Distributed System (of Systems).	SESAR1 WP14
SWIM Profile Assertion (SPA)	Declaration of the existence of a SWIM Profile combined with precisions on scope and motivation and with design considerations.	SESAR1 WP14
SWIM Purple Profile <Internal service binding> interface binding	SWIM Interface binding of type <Internal service binding> and included in the SWIM Purple Profile Technical Specification.	PJ.17-01
SWIM Purple Profile <Service binding> interface binding	SWIM Interface binding of type <Service binding> and included in the SWIM Purple Profile Technical Specification.	PJ.17-01
SWIM Purple Profile interface binding	SWIM Interface binding included in the SWIM Purple Profile Technical Specification.	PJ.17-01
SWIM Service	A “Service” designed in accordance with SWIM principles and applying the Working Method on Services.	B.04.03 D102 SESAR Working Method on Services
SWIM Technical Infrastructure (SWIM-TI)	The SWIM Technical Infrastructure (SWIM-TI) contributes to the services’ solution, aspects providing means supporting effective and secure ATM-specific service provision and consumption among SWIM-	SESAR1 WP14

Company General Use

	enabled ATM systems.	
SWIM-TI Administrative Console	Any application allowing authorized users to manage or control one or more SWIM Functions. Technical details of such consoles depend on implementation choices (e.g. CLI or graphical interfaces) but each console shall guarantee a certain level of security and compliance with current regulations.	SESAR1 WP14
SWIM-TI Solution	Software and Hardware representing the implementation of (applicable) SWIM-TI Technical Specifications.	SESAR1 WP14
Symmetric Key Cryptography (algorithms)	A Symmetric Key algorithm uses the same cryptographic key (shared secret key) for both encryption of plaintext and decryption of cipher text.	SESAR1 WP14
System of systems (SoS)	System of systems (SoS) is the viewing of multiple, dispersed, independent systems in context as part of a larger, more complex system. A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole.	SESAR1 WP14
System Port	A System Port is an interface provided by a Technical System. A System Port Connector asserts that a connection exists between two System Ports. Guidance: System ports are linked to Technical Systems that implement them. One System Port can be attached to many Technical Systems and one Technical System can have many System Ports. In addition, the System Ports can also be linked to the Capability Configurations that contain the Technical Systems to create views that describe technical interactions between Capability Configurations. System Ports and System Port Connectors are used to describe in detail the physical communication means used to transport the data from one system to another. To do so, the following elements are involved: a) System Port specification, defining the ports on each system and the protocols/standards relevant for the port (HTTP, SOAP, TCP, IP, etc.) b) Technical System to System Port connectivity defined as a System Port Connector, i.e., the communication link between two system ports, which is enabled by a specific Communication system. Multiple System Ports and System Port Connectors can be used to specify the communication/network	EATMA

Company General Use

	pathways through which systems interface.	
Technical Interoperability	An aspect of interoperability which covers the technical aspects of linking information systems. It includes topics such as interface specifications, interconnection services, data integration services, and data presentation and exchange.	SWIM Foundation
Technical Status	Indicates whether the SWIM Node or an element of the SWIM Node is working.	SESAR1 WP14
Technical System	A collection of Functional Blocks or Functions. Guidance: Technical Systems are artefacts that represent the technical part of Capability Configurations and contain Functional Blocks. Interaction between Technical Systems can be described via Resource Interactions (normally for legacy exchanges) and via Services (normally, for new exchanges). Both interactions carry Data elements. A Technical System comprises a set of System Ports that are the part of the Technical System in charge of implementing such data exchanges. Technical Systems can be linked to Functions that represents what the Technical System does.	EATMA
Type A EFB software application	Type A applications are EFB applications whose malfunction or misuse have no safety effect. Type A applications: (a) may be hosted on either portable or installed EFBs; (b) do not require any approval (AMC 20-25/ FAA AC-120 §6.2.2.1);and (c) should follow guidance provided in AMC 20-25/ FAA AC-120 Appendix D, paragraph D.2.	EASA AMC 20-25/ FAA AC-120
Type B EFB software application	Type B applications are applications: (a) whose malfunction or misuse are limited to a minor failure condition; and (b) which do neither substitute nor duplicate any system or functionality required by airworthiness regulations, airspace requirements, or operational rules.	EASA AMC 20-25/ FAA AC-120

	Type B applications: (a) may be hosted on either portable or installed EFBs; (b) require an operational assessment as described in paragraph AMC 20-25/ FAA AC-120 6.2.2.2; and (c) do not require an airworthiness approval.	
X.509 certificates	In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.	SESAR1 WP14
XML Encryption	XML Encryption is a specification (by W3C recommendation) that defines how to encrypt the contents of an XML element. Note: W3C (World Wide Web Consortium) is the main standards organization for the world wide web.	SESAR1 WP14

Table 1: Glossary

2.7 Acronyms and Terminology

Term	Definition
A/C	Aircraft
A/G	Air/Ground
ABAC	Attribute Based Access Control
ACC	Air Traffic Control Centre
ACD	Aircraft Control Domain
ADD	Architecture Description Document
AIM	Aeronautical Information Management
AIRM	Aeronautical Information Reference Model
AIS	Aeronautical Information Services
AISD	Airline Information Services Domain
AIXM	Aeronautical Information eXchange Model
AMDAR	Aircraft Meteorological Data Relay

Company General Use

AMQP	Advanced Message Queuing Protocol
AOC	Airline Operations Centre
ARR-MEP	Asynchronous Request/Reply (Request/Response) Message Exchange Pattern (SWIM-TI TAD)
ATC	Air Traffic Control
ATM	Air Traffic Management
BCA	Bridge Certification Authority
CA	Certification Authority (in the context of PKI)
CBA	Cost Benefit Analysis
CC	Capability Configuration
CDP	CRLs Distribution Point
CLI	Command-line interface
COTS	Commercial Of The Shelf
CRL	(X.509) Certificate revocation list
CSP	Certificate Service Provider
EATMA	European ATM Architecture
ECRYPT	European Network of Excellence in Cryptology
EFB	Electronic Flight Bag
EN	Enabler
FAA	Federal Aviation Administration
FB	Functional Block
FDRMR-MEP	Fully Decoupled Request/Multi-Reply (Request/Multi-Response) Message Exchange Pattern (PJ17.01 TS)
FDRR-MEP	Fully Decoupled Request/Reply (Request/Response) Message Exchange Pattern (SWIM-TI TAD)
G/G	Ground/Ground
HMAC	Keyed-hash message authentication code or hash-based message authentication code

HMI	Human-machine interface
HTTP(S)	HyperText Transfer Protocol (Secure)
IANA	Internet Assigned Numbers Authority
ICD	Interface Control Document
IdM	Identity Management
IdP	Identity Provider
IdSP	Identity Service Provider
IGMP	Internet Group Management Protocol
INTEROP	Interoperability Requirements
IP	Internet Protocol
IRS	Interface Requirements Specification
IS	Industrial Support
ISRM	Information Service Reference Model
IT	Information Technology
JMS	Java Messaging Service
LDAP	Lightweight Directory Access Protocol
MEP	Message Exchange Pattern
MET	Meteo or Meteorological
MIME	Multipurpose Internet Mail Extensions
MLD	Multicast Listener Discovery
MQ	Message Queue
MT	Message Topic
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NFR	Non-Functional Requirement
NSV	NAF System View
OASIS	Organization for the Advancement of Structured Information

Company General Use

	Standards
OCSP	Online Certificate Status Protocol
OS	Operating System
OSED	Operational Service and Environment Definition
PENS	Pan-European Network Service
PKI	Public Key Infrastructure
PP	Purple Profile
PSPULL-MEP	Publish/Subscribe Pull Message Exchange Pattern (SWIM-TI TAD)
PSPUSH-MEP	Publish/Subscribe Push Message Exchange Pattern (SWIM-TI TAD)
QoS	Quality of Service
RA	Registration authority (in the context of PKI)
RBAC	Role Based Access Control
RFC	Request For Comments (Internet Engineering Task Force terminology)
RSA	Rivest Shamir Adleman
SAML	Security Assertion Markup Language
SESAR	Single European Sky ATM Research Programme
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SoS	System of Systems
SPA	SWIM Profile Assertion
SPR	Safety and Performance Requirements

SRR-MEP	Synchronous Request/Reply (Request/Response) Message Exchange Pattern (SWIM-TI TAD)
SSL	Secure Socket Layer
STI	Security Token Infrastructure
STS	Secure Token Service
SWIM	System Wide Information Management
SWIM-TI	SWIM Technical Infrastructure
TAD	Technical Architecture Description
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRL	Technology Readiness Level
TS	Technical Specification
TVALR	Technical validation activities report
UTC	Coordinated Universal Time [International Telecommunication Union (ITU)]
UUID	Universally Unique IDentifier
V&V	Verification and Validation
VA	Validation authority (in the context of PKI)
VPN	Virtual Private Network
WAN	Wide Area Network
WP	Work Package
WS	Web Services
XML	Extensible Markup Language
XSD	XML Schema Definition

Table 2: Acronyms and terminology

3 SESAR Solution Impacts on Architecture

3.1 Target Solution Architecture

3.1.1 SESAR Solution(s) Overview

PJ.17-01 technological solution contributes to one of the SESAR Key Features: ENABLING AVIATION INFRASTRUCTURE [23]. The SWIM-TI is the interoperable (runtime) infrastructure (ground/ground and air/ground) over which SWIM services are provided and consumed. It is an enabler for technical interoperability between SWIM services consumers and providers.

The main challenges in the context of the technical interoperability are fragmentation versus “one size does not fit all”. In SWIM these challenges are faced by profiling the SWIM-TI: all the technical interoperability needs of the System of Systems (SoS) are taken into consideration and segmented into groups for each of which a satisfactory uniform and standard based solution is defined (the SWIM Profiles).

The SWIM Profiles represent appropriate mandated solutions including the required SWIM Technical Infrastructure features, adopted standards, configurations and Quality of Services.

The first level of segmentation identified in the analysis of technical interoperability needs and constraints of the System of Systems (SoS) is the separation between Ground-Ground SWIM and Air-Ground SWIM segments.

The Ground-Ground SWIM segment is a set of Ground functions that allow Ground SWIM Enabled applications to interact via SWIM Services. This SWIM segment has been further segmented identifying the SWIM Yellow, Blue and Green profiles.

The Air–Ground SWIM segment is a set of Aircraft and Ground functions that allow Aircraft SWIM Enabled applications to interact with Ground SWIM Enabled applications via provisioning and consumption of SWIM Services. The SWIM Purple profile is covering the needs and constraints identified for this segment (a SWIM service designed, provided and consumed according to the Purple Profile is said Purple Profile enabled). In the context of SESAR 2020 PJ.17-01 the scope is restricted to Air/Ground advisory information sharing or Advisory Purple Profile Enabled SWIM Services (§2.6). Air/Ground safety-critical information sharing may introduce additional requirements that are not taken into account in this specification.

This aim of the Purple Profile for advisory information sharing is model via the SWIM Profile Assertion (SPA) provided in Appendix A.

Table 3~~Table 3~~ provides the SESAR Enablers relevant for the Purple Profile together with applicable functional blocks and EN coverage. The current analysis is based on the latest Data Set available in the SESAR Programme, specifically version “Data Set 19” (DS19).

SESAR Solution ID and Title	Functional Blocks/Role impacted by the SESAR Solution	Enabler ID (from EATMA)	Enabler Title (from EATMA)	Enabler coverage

	(from EATMA)			
PJ.17-01, SWIM-TI Purple Profile For Air/Ground Advisory Information Sharing	SWIM Messaging Purple Profile SWIM Security Purple Profile	SWIM-INFR-06b	Ground side SWIM technical infrastructure for Air-Ground Advisory Information Sharing	**Fully**
	SWIM Messaging Purple Profile SWIM Security Purple Profile	SWIM-INFR-06c	Air side SWIM technical infrastructure for Air-Ground Advisory Information Sharing	**Fully**

Table 3: SESAR Solution PJ.17-01 Scope and related Functional Blocks/roles & Enablers

This technical specification addresses following technical systems:

- Ground Purple Profile Technical System:
  - Enabler: SWIM-INFR-06b
  - Brief description: The Air–Ground SWIM segment is a set of Aircraft and Ground functions that allow Aircraft SWIM Enabled applications to interact with Ground SWIM Enabled applications via provisioning and consumption of SWIM Services. At technical view level, the component that provides/realizes/deploys such functions is the SWIM Node. The Ground Purple Profile Technical System consists of the Ground Purple Profile SWIM Node covering ground side functions of the Air–Ground SWIM for advisory information sharing (SYS EN SWIM-INFR-06b).
- Air Ground Purple Profile Technical System:
  - Enabler: SWIM-INFR-06c
  - Brief description: The Air–Ground SWIM segment is a set of Aircraft and Ground functions that allow Aircraft SWIM Enabled applications to interact with Ground SWIM Enabled applications via provisioning and consumption of SWIM Services. At technical view level, the component that provides/realizes/deploys such functions is the SWIM Node. The Air Purple Profile Technical System consists of the Air Purple Profile SWIM Node covering aircraft side functions of the Air–Ground SWIM for advisory information sharing (SYS EN SWIM-INFR-06c).

In §3.1.1.2 relevant use cases, the relationships with SWIM service (service provider/consumer roles, messaging entities, interface bindings, etc.) are described. Architectural views are specified in §4.

3.1.1.1 Deviations with respect to the SESAR Solution(s) definition

None.

3.1.1.2 Relevant Use Cases

The Purple Profile technical systems are the interoperable (runtime) infrastructure over which Advisory Purple Profile enabled SWIM services are provided and consumed by air and ground Purple Profile enabled technical systems[1].

This specification is not limiting or describing the operational view (SPR-INTEROP/OSED) of the SWIM services provided over the Air-Ground SWIM segment. In other words, this specification is not defining or constraining, from an operational point of view, which advisory information should be shared via the Purple Profile.

The Purple Profile is designed applying following principles:

- It is possible to identify needs/constraints common to all the Advisory Purple Profile Enabled SWIM Services irrespective of the analysis of the specific services. This is possible due to the fact that only Air/Ground advisory information sharing is in scope of this solution. These common needs/constraints are identified combining both bottom up and top-down inputs and used to design the Purple Profile.
- Taking into account that different Advisory Purple Profile Enabled SWIM Services may have different functional and non-functional service level requirements, the Purple Profile is designed to support flexible configuration of the Purple Profile interface bindings especially in terms of MEPs, information security and QoS.

This approach is in line with SWIM profiles principles (fragmentation versus “one size does not fit all”): all the technical interoperability needs of the System of Systems (SoS) are taken into consideration and segmented into groups for each of which a satisfactory uniform and standard based solution is defined. The latter (i.e. the Purple Profile) represents appropriate mandated solution including the required SWIM Technical Infrastructure features, adopted standards, configurations and Quality of Services.

Taking into account the above, it is possible to describe relevant operational use cases by referring to a generic Purple Profile enabled SWIM service and describing the artefacts and the technical options the Purple Profile offers when designing and instantiating the service.

Purple Profile and Purple Profile enabled SWIM Services

The Purple Profile provides, among others, specific interface requirements of type “Service Binding” (linked with EATMA System Port). A “Service Binding” (refer to §C.1.1) defines the protocol stacks for accessing Purple Profile enabled SWIM services (interface bindings are further detailed in §4.2.2). These are the primary (and SWIM service independent) access specifications for the technical design of SWIM services: a SWIM Service interface specification consists mainly in choosing a “Service Binding” and complementing it with service specific design artefacts (e.g. XSD, detailed technical provision schema). Among others, the interface bindings include also *security* field aiming at enumerating for each security need of a defined set, the location of the security control or the

[1]According to EATMA interaction between technical systems can be described via Resource Interactions (normally for legacy exchanges) and via Services (normally, for new exchanges).

security controls, that will support the security need in the binding. The defined set of security controls consists of Confidentiality, Integrity, Authentication, Authorization, Non-repudiation.

The Purple Profile defines also specific constraints based on Air-Ground SWIM specificities and architecture. In particular the Purple Profile provides also:

- Technical architecture and messaging federation to integrate the Aircraft information system in SWIM and allowing the provision/consumption of services,
- Configuration aspects linked to service specific interface bindings and technical architecture.

In other words, a SWIM service consumed or provided over the Purple Profile consists not only of the chosen interface binding but also of the technical provision/consumption architecture and service specific configurations.

Within the EATMA Service layer, Services have one or more Service Interfaces and the latter represent the mechanism by which a service communicates. When creating design models of Services, a distinction is often made between the Service Interface and the Service Interface Definition. The Service Interface is the actual endpoint (port) by which the Service communicates while the Service Interface Definition is the specification of the interface.

The Purple Profile provides a set of Service interface bindings, together with infrastructure architecture and configuration aspects, allowing Service architects to design Service Interface Definitions for Air-Ground SWIM. Taking into account that a service may be composed by more than one interface, multiple and potentially different interface bindings (one for each service interface) may be selected when designing the Service (Service Interface definitions).

The SWIM Profiles bindings are standard based protocol stack (technical interoperability) and are SWIM service agnostic: each binding includes a “contract”[2] field that specifies or refers to design artefacts that have to be provided according to the specific service (e.g. XSD for Data Elements, actual service network endpoint(s), QoS, etc.).

Each service binding supports one or more MEPs: in the SWIM context, the MEPs are used to design the SWIM service interfaces and to characterize the SWIM-TI messaging and interface bindings. Primarily objective of the SWIM-TI MEPs catalogue [Appendix B] is to provide primitive MEPs situated at the perimeter between SWIM-TI layer and Application layer. MEPs can be emulated on top of one or more layers each providing one or more other MEPs. Primitive MEPs can be composed to realize more complex MEPs.

As part of the SWIM service design thread, the MEPs are primarily used to model, in a technology independent way, the end-to-end message exchange behaviour at service interface level. It is then part of the SWIM service technical design phase to conduct the identification of SWIM-TI interface binding that better fits the purpose of a given SWIM service interface.

[2] The term “contract” has not to be confused with the contract datalink mode. In both cases this term is not used alone and in particular, for the interface bindings, it is used as “contract field of the interface binding”.

The provided MEPs are intended as end to end behaviour at application/service/service interface level. The expected end to end behaviour can be then realized over the Purple Profile by properly composing/realizing the MEPs at infrastructure level.

Starting from the available MEPs and taking into account that both uplink and downlink information sharing are required, it is possible to identify the technical use cases in Table 4. The use cases refer to a *SWIM service over a "MEP"* and the semantic is as follows:

- *Request/Response SWIM service*: it is a SWIM service as defined by EATMA whose interface has been designed using MEPs belonging to the Request/Response MEPs family.
- *Publish/Subscribe SWIM service*: it is a SWIM service as defined by EATMA whose interface has been designed using MEPs belonging to the Publish/Subscribe MEPs family.

It is important to notice that even if the use cases refer to SWIM service over a "MEP", the right level of granularity is the SWIM service interface level (during SWIM service design MEPs are assigned to all service interfaces).

UC ID	UC Title	Aircraft role	Ground-based system role	Uplink / Downlink	MEP Family	Brief description
PPUC-01a	Aircraft initiated Request/Response information exchange	Consumer	Provider	Uplink	Request/Response	An aircraft consumes a Request/Response SWIM service provided by a ground-based system (FDRR-MEP).
PPUC-01b	Aircraft initiated Request/Multi-Response information exchange	Consumer	Provider	Uplink	Request/Response	An aircraft consumes a Request/Multi-Response SWIM service provided by a ground-based system (FDRMR-MEP).
PPUC-02	Ground-based system provided Publish/Subscribe information exchange	Consumer	Provider	Uplink	Publish/Subscribe	An aircraft consumes a Publish/Subscribe SWIM service provided by a ground-based system (PS*-MEP).
PPUC-03a	Ground-based system initiated Request/Response information exchange	Provider	Consumer	Downlink	Request/Response	A ground-based system consumes a Request/Response SWIM service provided by an aircraft (FDRR-MEP).

UC ID	UC Title	Aircraft role	Ground-based system role	Uplink / Downlink	MEP Family	Brief description
PPUC-03b	Ground-based system initiated Request/Multi-Response information exchange	Provider	Consumer	Downlink	Request/Response	A ground-based system consumes a Request/Multi-Response SWIM service provided by an aircraft (FDRMR-MEP).
PPUC-04	Aircraft provided Publish/Subscribe information exchange	Provider	Consumer	Downlink	Publish/Subscribe	A ground-based system consumes a Publish/Subscribe SWIM service provided by an aircraft (PS*-MEP).

Table 4: SWIM Purple Profile technical use cases

These use cases aim at describing at high level the specific MEPs (end to end behaviour) in the Air-Ground SWIM context without distinguishing, at this level, nominal and non-nominal cases.

In §4 these technical use cases are analysed and detailed in terms of technical architecture and requirements and, for each of them, both run-time and configuration time aspects are described. Both use cases analysis and design are based on the messaging characterization in Appendix B where both nominal and non-nominal cases are characterized.

In Figure 1, a schematic representation of the relationship between the SWIM Services and the Purple Profile is provided. The diagram explains the relationship between Technical Systems, Service and Purple Profile Service Bindings. The diagram is Purple Profile technical architecture and architecture options agnostic.

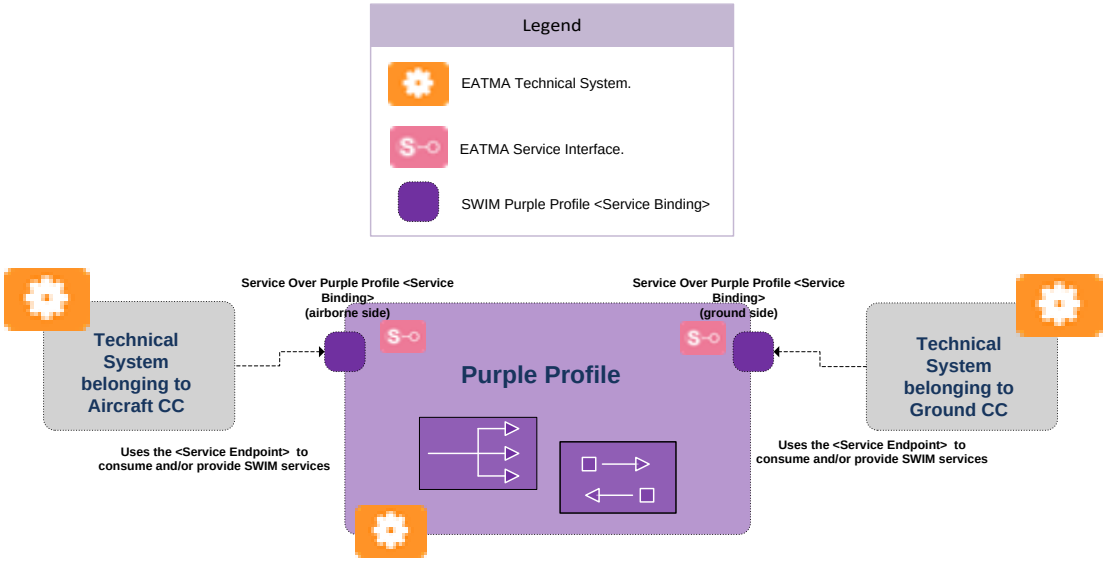


Figure 1: SWIM Purple Profile and SWIM Services (conceptual)

The design artefacts characterizing a SWIM Service over the Purple Profile are:

- Pair of aircraft and ground «Service Binding» used to consume/provide the service. This specification provides options for the bindings and the design is driven by the use cases described in Table 4. For instance, for a *Publish/Subscribe SWIM service* (consumed or provided by Aircraft CC's Technical Systems) a set of aircraft and ground «Service Binding» options supporting the Publish/Subscribe MEP are described in this specification. During the SWIM Service design, the appropriate «Service Binding» pair is chosen.
- Service specific artefacts describing the «contract» field of the selected «Service Binding» pair.
- Purple Profile Messaging Technical architecture and related configuration aspects. A secure and reliable federated messaging infrastructure (aircraft and ground) is designed to allow the Aircraft to "participate to SWIM" according the applicable MEPs (infrastructure level messaging between the pair of aircraft and ground «Service Binding») and SWIM services configuration (e.g. addressing, QoS, etc.).

OSED for aeronautical information (AIS) and meteorological (MET) data link services

As anticipated above it is not strictly required to derive the Purple Profile design from specific SESAR2020 SPR-INTEROP/OSED related to Air-Ground SWIM. The identified technical used cases and the Purple Profile flexibility (interface bindings catalogues and interface binding contract field) are considered enough to cover the needs for any advisory air/ground information sharing. It is however considered interesting to complement this analysis by assessing any relevant SPR-INTEROP/OSED.

As an operational guideline, a standard OSED could be evaluated: the EUROCAE/RTCA ED-151/DO-308 (OSED for aeronautical information (AIS) and meteorological (MET) data link services).

The ED-151 [37] defines several operational data link modes (independent of the specific service) that may be used for exchanging AIS and MET information. As the specific AIS and MET service design could also consist of a hybrid of the described modes (e.g. downlink service with both time-

controlled distribution and Demand (ground initiated) mode), these modes are considered as key building modes for operational services relying on data exchanges. Thus, the data link modes are considered valuable in this solution because it is a way to characterize the patterns the infrastructure is expected to enable.

The definitions of these operational data link modes, extracted from ED-151 Appendix A [37], are provided in Table 5.

Data link mode	Description
Broadcast	The data transmission to any number of unspecified users within the operating volume of the transmitter who have the equipment to receive the transmission. This transmission may be on a single channel or multiple channels carrying all or part of the transmitted data. PJ.17-01 guidance: even if the description of the mode seems to be at lower level with respect to Demand and Contract modes, in accordance with ED-151 the broadcast mode is applicable to information exchange level.
Demand	The Demand mode defines a method for the aircraft to request specific information and for the ground system to provide the aircraft with the requested information.
Contract	The Contract mode defines a method for the aircraft to request specific information and for the ground system to provide the aircraft with this information and any updates to this information until the contract is terminated.

Table 5: ED-151 Data link modes

Even if the definitions of the three modes refer to uplink exchange, they could also be used for both downlink and crosslink exchanges. ED-151 extracted texts supporting this consideration are provided here below:

- **Downlink**: *The downlink mode supports the transmission of meteorological information from an aircraft to the ground. Downlink transmissions are automated and may occur on a time-controlled, altitude-controlled, distance-controlled basis or be event-driven. The basis for the occurrence of downlink transmissions is normally pre-programmed but may be specified (or changed) through a ground initiated Demand request if a command and control capability has been established*.
- **Crosslink**: *The crosslink mode supports the transmission of meteorological information from an aircraft to other aircraft in the vicinity. Depending on the communications architecture, crosslink transmissions may be synonymous with a combination of downlink and uplink transmissions rather than independent transmissions*.

However, direct aircraft to aircraft information exchanges are considered local and thus outside SWIM. If information provided by one aircraft shall be consumed by another aircraft in a SWIM-

compliant way, it has to go through the ground SWIM infrastructure. Such information exchange is a combination of downlink and uplink exchanges.

The ED-151 data link modes describe end-to-end behaviour (application/service layer) and conceptually they are related to the MEPs introduced above. In particular, from technical interoperability point of view (Purple Profile's scope) it is possible to realize the datalink modes via one or more MEPs. This solution assessed different options and the those considered effective and feasible are reported in Table 6.

In accordance with above considerations, the provided MEPs are intended as end to end behaviour at application/service/service interface level. The expected end to end behaviour can be then realized over the Purple Profile by properly composing MEPs at infrastructure level.

Data link mode	MEP/MEP Family	Note/Clarification
Broadcast	Publish/Subscribe Push (PSPUSH-MEP)	
Demand	Request/Response (FDRR-MEP)	This is the recommended option for demand data link mode because the FDRR-MEP natively supports what is required.
Contract	Request/Multi-Response (FDRMR-MEP)	This is the recommended option for contract data link mode because the FDRMR-MEP natively supports what is required.
	Request/Response (FDRR-MEP) composed with Publish/Subscribe (PS*-MEP)	The contract data link mode can be realized by composing the provided MEPs: the FDRR-MEP is used for retrieving current information and the PS*-MEP to receive updates. The updates can be received asynchronously (PSPUSH-MEP) or fetched synchronously (PSPULL-MEP).

Table 6: ED-151 Data link modes and SWIM-TI MEPs/MEP families

The data link modes can be now easily linked to the SWIM Purple Profile technical use cases (and related design and requirements) using the MEP/MEP family as key. For instance, the contract datalink mode for uplink can be realized:

- by composing the solutions specified for PPUC-01a and PPUC-02, or
- by using the solutions specified for the PPUC-02.

3.1.1.3 Applicable standards and regulations

This section identifies the list of standards and regulations that are applicable to the SESAR Solution PJ.17-01.

1. ISO/IEC 19464:2014 Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification, First Edition 2014-05-01 http://standards.iso.org/ittf/PubliclyAvailableStandards/c064955_ISO_IEC_19464_2014.zip.
2. IETF RFC 793 Transmission Control Protocol September 1981 http://tools.ietf.org/html/rfc793
3. IETF RFC 791 Internet Protocol September 1981 http://tools.ietf.org/html/rfc791
4. IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification December 1998 http://tools.ietf.org/html/rfc2460
5. IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2 August 2008 http://tools.ietf.org/html/rfc5246
6. IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 August 2018 https://tools.ietf.org/html/rfc8446
7. IETF RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0 March 2011 http://tools.ietf.org/html/rfc6176
8. IETF 2616 Hypertext Transfer Protocol -- HTTP/1.1 June 1999 http://tools.ietf.org/html/rfc2616
9. IETF informational RFC 2818 HTTP Over TLS May 2000 http://tools.ietf.org/html/rfc2818
10. W3C Recommendation Extensible Markup Language (XML) 1.0 (Fifth Edition) 26 November 2008 http://www.w3.org/TR/xml/
11. W3C Recommendation Extensible Markup Language (XML) 1.0 (Fourth Edition) 16 August 2006, edited in place 29 September 2006 http://www.w3.org/TR/2006/REC-xml-20060816/
12. W3C Recommendation XML Schema Part 1: Structures Second Edition 28 October 2004 http://www.w3.org/TR/xmlschema-1/
13. W3C Recommendation XML Schema Part 2: Datatypes Second Edition 28 October 2004 http://www.w3.org/TR/xmlschema-2/
14. IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP June 2013 http://tools.ietf.org/html/rfc6960
15. IETF RFC 4510 Proposed Standard, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006 http://www.rfc-editor.org/rfc/rfc4510.txt
16. IETF RFC 5280 Proposed Standard, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 http://www.rfc-editor.org/rfc/rfc5280.txt
17. IETF RFC 4523 Proposed Standard, Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates, June 2006 http://www.rfc-editor.org/rfc/rfc4523.txt
18. IETF RFC 4158 Internet X.509 Public Key Infrastructure: Certification Path Building September 2005 http://tools.ietf.org/html/rfc4158

19. IETF RFC 6434, Memo, IPv6 Node Requirements, December 2011 http://tools.ietf.org/html/rfc6434
20. IETF RFC 950, Internet Standard, Internet Standard Subnetting Procedure, August 1985 http://tools.ietf.org/html/rfc950
21. IETF RFC 4033 Domain Name System Security Extensions (DNSSEC), March 2005 https://tools.ietf.org/html/rfc4033.
22. Security Requirements for Cryptographic Modules US Federal Information Processing Standard (FIPS 140-2), May 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
23. IETF RFC 7568 Deprecating Secure Sockets Layer Version 3.0, June 2015 https://tools.ietf.org/html/rfc7568.
24. ISO/IEC 25010:2011 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models, edition 1, March 2011 https://www.iso.org/standard/35733.html.
25. EUROCAE ED-151 - Operational Services and Environment Definition (OSED) for Aeronautical Information Services (AIS) and Meteorological (MET) Data Link Services, December 2007.
26. IETF RFC 1122 Internet Standard, Requirements for Internet Hosts Communication Layers, October 1989 http://tools.ietf.org/html/rfc1122.
27. IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) August 2001 http://www.rfc-editor.org/rfc/rfc3161.txt.
28. IETF RFC 5652 Internet Standard, Cryptographic Message Syntax (CMS), September 2009 http://www.rfc-editor.org/rfc/rfc5652.txt.
29. RSA Laboratories PKCS #12 v1.1: Personal Information Exchange Syntax, October 27, 2012 Standard http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm.
30. IETF RFC 2046 Multipurpose Internet Mail Extensions (MIME) Media Types https://www.ietf.org/rfc/rfc2046.txt.
31. IETF RFC 1952 GZIP file format specification version 4.3 https://www.ietf.org/rfc/rfc1952.txt.
32. IETF RFC 1951 DEFLATE Compressed Data Format Specification version 1.3 https://www.ietf.org/rfc/rfc1951.txt.
33. IETF RFC 1950 ZLIB Compressed Data Format Specification version 3.3 https://www.ietf.org/rfc/rfc1950.txt.
34. IETF RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace https://www.ietf.org/rfc/rfc4122.txt.
35. IETF RFC 3986 Uniform Resource Identifier (URI), Generic Syntax https://www.ietf.org/rfc/rfc3986.txt.
36. ISO/IEC 42010:2011 Systems and software engineering -- Architecture description, December 2011, https://www.iso.org/standard/50508.html.
37. AMC 20-25 Airworthiness and operational consideration for Electronic Flight Bags (EFBs), ED Decision 2014/001/R

38. ARINC REPORT 660B CNS/ATM AVIONICS ARCHITECTURES SUPPORTING NEXTGEN/SESAR CONCEPTS, January 10, 2014
39. ARINC REPORT 821 AIRCRAFT NETWORK SERVER SYSTEM (NSS) FUNCTIONAL DEFINITION, December 9, 2008
40. ARINC CHARACTERISTIC 763-2 NETWORK SERVER SYSTEM, NOVEMBER 21, 2001
41. ARINC SPECIFICATION 834-7 AIRCRAFT DATA INTERFACE FUNCTION (ADIF), August 9, 2017
42. ARINC REPORT 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK, December 20, 2005
43. ARINC REPORT 852 GUIDANCE FOR SECURITY EVENT LOGGING IN AN IP ENVIRONMENT, June 21, 2017
44. ARINC REPORT 842-1 GUIDANCE FOR USAGE OF DIGITAL CERTIFICATES, December 12, 2013
45. ARINC SPECIFICATION 823P2 DATALINK SECURITY PART 2 – KEY MANAGEMENT, March 10, 2008
46. EUROCAE ED-175 - Safety and Performance Requirements (SPR) for AERONAUTICAL INFORMATION SERVICES (AIS) and METEOROLOGICAL (MET) DATA LINK SERVICES, January 2011.

3.1.2 Capability Configurations required for the SESAR Solution

In the table below the Capability Configurations (CCs) required by the SESAR Solution are provided together with the relevant (sub)-Operating Environments where the CCs operate, and the links between CCs and Capabilities, Nodes and Stakeholders.

SESAR Solution ID and Title	Capability Configurations (CCs) (from EATMA)	Sub-Operating Environment(s) where the CCs operate	Capabilities (from EATMA)	Nodes (from EATMA)	Stakeholders (from EATMA)
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	SWIM Identity Management	Airport (Note 1), TMA, En-Route (a)	SWIM support		Civil SWIM Service Provider
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	Civil Aircraft	Airport, TMA, En-Route	Execute Trajectory SWIM-based Information Dissemination	Flight Deck	Airspace User
PJ.17-01 SWIM-TI	Civil AU	Airport, TMA,	SWIM-based	Airspace User	Airspace

Company General Use

Purple Profile for Air/Ground Advisory Information Sharing	Operations Centre	En-Route	Information Dissemination	Operations	User
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	TWR	Airport, TMA, En-Route	Meteorological Observation and Forecasting Provision	Aerodrome ATS	Civil ATS Aerodrome Service Provider
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	Aerodrome ATM-MET	Airport, TMA, En-Route	Meteorological Observation and Forecasting Provision	Meteorological Service Provision	Civil MET Service Provider
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	Regional AIM	Airport, TMA, En-Route	Aeronautical and Meteorological Information Management	Aeronautical Information Service Provision	Network Manager
PJ.17-01 SWIM-TI Purple Profile for Air/Ground Advisory Information Sharing	ATM-MET	Airport, TMA, En-Route	Meteorological Observation and Forecasting Provision	Meteorological Service Provider	Civil MET Service Provider

Table 7: List of Capability Configuration required for the SESAR Solution

Note 1: A/C Digital identity information configuration/maintenance is only operated in "Airport" environment.

Currently for the ATM-MET CC only the node "*Meteorological Service Provider*" is linked. This CC may also consume aircraft provided weather observation (aircraft provided service like AMDAR [50]).

It is anticipated that the above are bottom-up considerations. It is up to the concerning ATM solutions to identify and design advisory information exchange services and to identify concerned CCs accordingly (e.g. AIM information may be also distributed via a SWIM service belonging to the National AIM).

3.2 Changes imposed by the SESAR Solution on the baseline Architecture

All the relevant changes identified in TRL6 have been already submitted as Change Requests (CRs) during DS19 preparation. The changes can be summarized as follows:

- The POI Step POI-0017-IS has been created connecting the PJ.17-01 solution to relevant ENs.
- In order to distinguish between air and ground Purple Profile
  - The existing SYS EN (SWIM-INFR-06b) definition has been updated restricting its scope to ground side Purple Profile. This EN encompasses the creation of the Ground Purple Profile technical system, its FBs, its Functions and its System Ports.
  - A new SYS EN ((SWIM-INFR-06c) has been created restricting its scope to air side Purple Profile. This EN encompasses the creation of the Air Purple Profile technical system, its FBs, its Functions and its System Ports.

Enabler ID (from EATMA)	Enabler Title (from EATMA)	Changes

Table 8: List of changes due to the SESAR Solution

4 Technical Specifications

This chapter aims at describing the Purple Profile architecture in terms of concept, architecture design and requirements. Entry-level overview of the Purple Profile is provided in §3.1.1. In particular, in that section the relationships with SWIM service (service provider/consumer roles, messaging entities, interface bindings, etc.) are described. These relationships and concepts are used and detailed in this chapter.

In order to describe the Purple Profile architecture in a structured manner, the ISO/IEC/IEEE 42010:2011 standard is adopted in this TS. In particular different actors[3] (i.e. "stakeholders" in ISO/IEC/IEEE 42010:2011), concerns, architecture viewpoints and architecture views are identified and described. The viewpoints are based on the following SWIM-TI aspects:

- "What": this aspect deals with tailoring of the overall SWIM-TI functional view (EATMA functional blocks) according to the Purple Profile technical systems use cases and purpose.
    - Example of what: "*The SWIM-TI Message Routing shall provide message level subject-based routing relying on message properties.*".
    - Anti-pattern example: "*The SWIM-TI shall allow to detect known vulnerabilities*". Even if this requirement is about what the SWIM-TI shall do, it should be part of the "how good" (security NFR) because there is no "vulnerabilities detection" function as part of the SWIM-TI functional view.
- "How": this aspect deals with technical realization of functions (the "what") according to technical interoperability needs assessment. In particular, the "how" is specified only when interoperability needs have been identified:
    - Example of how: realization of the message routing using AMQP 1.0 *to*, *from* and *subject* fields.
    - Anti-pattern: to specify the "how" about the requirement "*The SWIM-TI Message Routing shall allow routing by enforcing Routing Policy.*" may not be necessary because it could be considered as an internal detail of the SWIM Node implementation. In particular how this is realized in not impacting technical interoperability.

  The "how" specializes ("how" a given "what" is realized) and complements (the how is only provided when interoperability needs have been identified) the "what":

  specialization semantics: a requirement about the "how" specializes a requirement about the "what". Implementations conformant to the requirement(s) specifying the "how" are by definition conformant to the requirement about the "what".

  complement semantics: a requirement about the "how" could not satisfy any requirement about the "what". A requirement about the "what" could not be satisfied by any

[3] The term actor is used to avoid confusion with (ATM) "Stakeholder" as defined in EATMA.

requirement about the "how". Implementations are expected to be conformant also to these requirements.

- "How good": this aspect deals with the NFRs concerning the functions ("what"), technical realization of the functions ("how") and overall SWIM Node.
  - *"Evidence of the correct execution of security functions shall be provided in the form of either an acknowledgement or auditing."*.
  - *"The messaging level infrastructure shall support a minimum and maximum value of idle-timeout at between 60 seconds and 600 seconds."*.
  - *"The SWIM Node Continuous unavailability shall be as follows:*

    Measurement: <= 20 minutes

    …".
- "Where": this aspect deals with deployment options of elements concerning the "what" and "how" aspects.

Figure 2 provides a graphical representation of the relationships between above aspects.

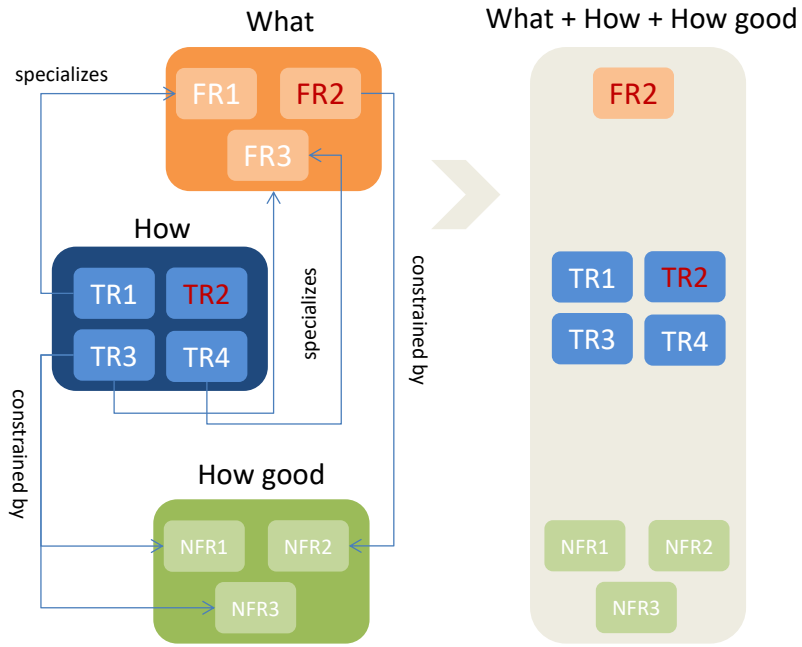


Figure 2: What, How and How good aspects relationships

Figure 2 indicates functional (FR*), technical (TR*) and non-functional (NFR*) requirements a conformant implementation covers. Requirements FR1 and FR2 are by definition covered in case the implementation covers TR1, TR3 and TR4. Furthermore, it could happen that when dealing with the "how", requirements (e.g. TR2 in Figure 2) not directly traceable to the "what" could be identified. In case, this has to be justified:

- The requirement is linked to/derived from other requirements concerning the "how".
- The requirement is linked to/derived from design decisions/constraints at technological level.

Purple Profile Viewpoints overview

Viewpoints adopted to describe the Purple Profile architecture are the following:

- **Functional Viewpoint** which addresses the "what" without dealing with the "where" or "how" aspects of the SWIM-TI. It mainly addresses the concern about what the Purple Profile technical systems shall/should/could do. The concern is described in terms of identification of applicable EATMA SWIM-TI functions and functional requirements. The functional viewpoint is described in the Purple Profile Functional view §4.2.1 and it is based on the messaging characterization in Appendix B. Requirements concerning this view are provided in §4.3.1. In order to allow this view to persist and remain valid across technology changes, it is expected to be independent of and totally silent about specific technology.
- **Technical Viewpoint** which complements and specializes the "what" aspect addressing the "how" and "how good" but without dealing with the "where" aspect of the SWIM-TI. It provides the technical view according to technical architecture and technical interoperability needs ("how") and SWIM-TI's NFRs ("how good"). It mainly addresses the concern about how to realize the sub-set of functions according to interoperability needs assessment. The technical viewpoint is described in the Purple Profile Technical view in §4.2.2. Requirements concerning this view are provided in §4.3.2-§4.3.7.
- **Deployment Viewpoint** which mainly addresses the concern about how to deploy the ("what" and "how" of) Purple Profile. It provides deployment options addressing the "where" in terms of architecture technical and integration options. This specification does not impose/restrict the deployment options. Furthermore, the list of deployment options is not supposed to be complete and exhaustive. The deployment viewpoint is described in the Purple Profile Deployment view in §4.2.3.

Taking into account the needs to contribute to EATMA architecture view applying EATMA defined guidance, terminology and model and that EATMA model and concerns do not fit the above mentioned views, an additional viewpoint is needed:

- **EATMA Viewpoint** which provides the EATMA architecture view according to EATMA model and EATMA concerns. It mainly put together in different EATMA diagrams, relevant (according to EATMA guidance) elements from functional and technical views (e.g. functions from functional view and system ports from technical view).

It is anticipated that the EATMA Viewpoint does not add additional information to the 3 main viewpoints: it applies EATMA model targeting the concerns linked to EATMA.

The relationships between the three main viewpoints is similar to the ones described above when introducing the "what", "how", "how good" and "where" aspects. Additional details concerning each viewpoint are provided in §4.2.

4.1 Functional architecture overview

This sections provides Purple Profile EATMA architecture view (concerning the EATMA viewpoint) according to EATMA model and EATMA concerns. It mainly put together, in different EATMA diagrams, relevant (according to EATMA guidance) elements from functional and technical viewpoints (e.g. functions from functional viewpoint and system ports from technical viewpoint).

Some diagrams may be not readable due to limitation of the layout: all the NAF views are however available in EATMA.

The EATMA viewpoint is described according to SESAR2020 TS template and EATMA guidance. It is anticipated that what provided in this section is a proper consolidation of aspects detailed in §4.2. The identification/documentation of concerns related to EATMA diagrams is out of scope of this document. The primary actor addressed by this viewpoint is “PPArchA04” (“EATMA architect”) representing any EATMA expert interested in understanding/assessing the Purple Profile technical systems according to EATMA defined diagrams and elements.

There are a number of PJ.17-01 aspects depending on deployment, technical and service design options. All these “options” are described in §4.2.2 and §4.2.3. NAF views provided in the sections are for illustrative purposes and they are not exclusive in terms of technical and deployment options. However, the NAF view are representative of the use of Purple Profile:

- Illustrative NSV-1 including one uplink MET service (e.g. METAR) and one downlink MET service (MET report).
- Illustrative NSV-1 including one uplink AI service (e.g. D-NOTAM, IDB).
- Illustrative NSV-2 concerning the MET NSV-1.
- NSV-4 views describing:
    - Uplink MET over PS-MEP (both subscription management and publication).
    - Uplink MET over FDRR-MEP.
    - Downlink MET over PS-MEP (both subscription management and publication).

The next diagrams represent the functional decomposition of both technical systems: SWIM Purple Profile Ground and SWIM Purple profile Air. Artifact Structure Diagram is the logical grouping of functional blocks encompassed by the technical system. Artifact Assembly Diagrams list the owned EATMA system ports and the service interface logical ports, and service provisioning through the link between system ports and service points. In accordance with §4.2.2.3, OCSP and CDPs system ports are optional and mandatory only when claiming conformance to <PP Ground Security+> or/and <PP Air Security+> profile parts.

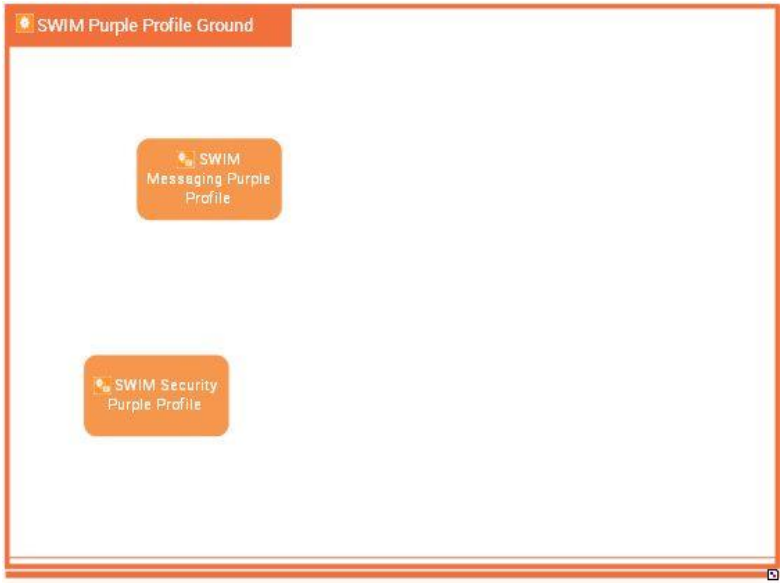


Figure 3: Artifact Structure Diagram - SWIM Purple Profile Ground

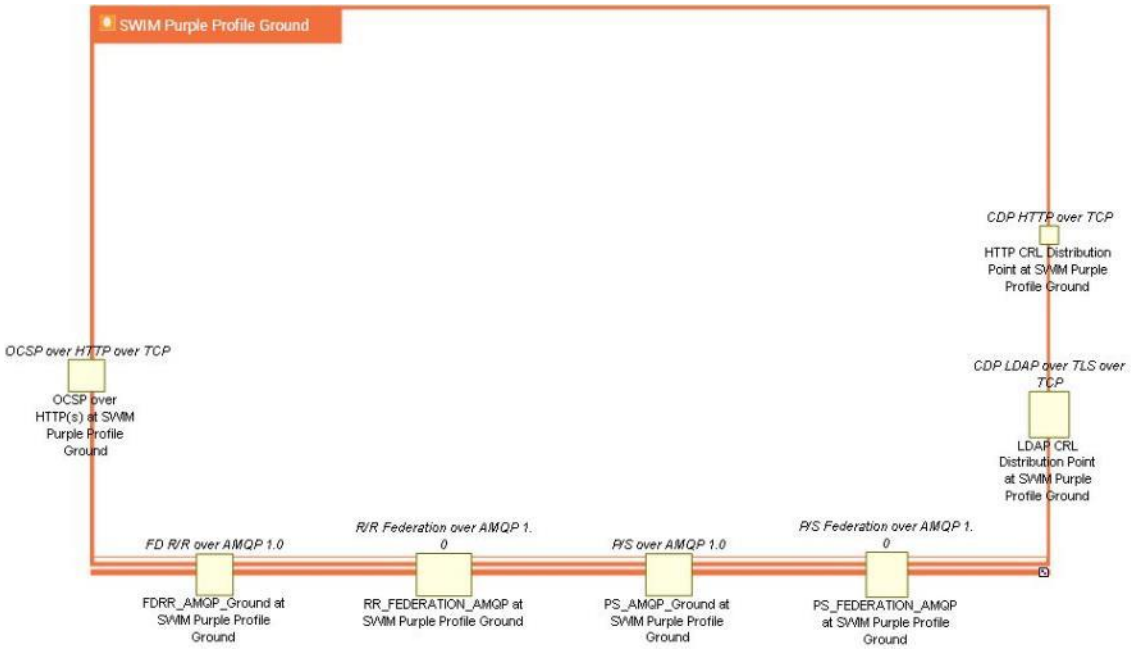


Figure 4: Artifact Assembly Diagram - SWIM Purple Profile Ground

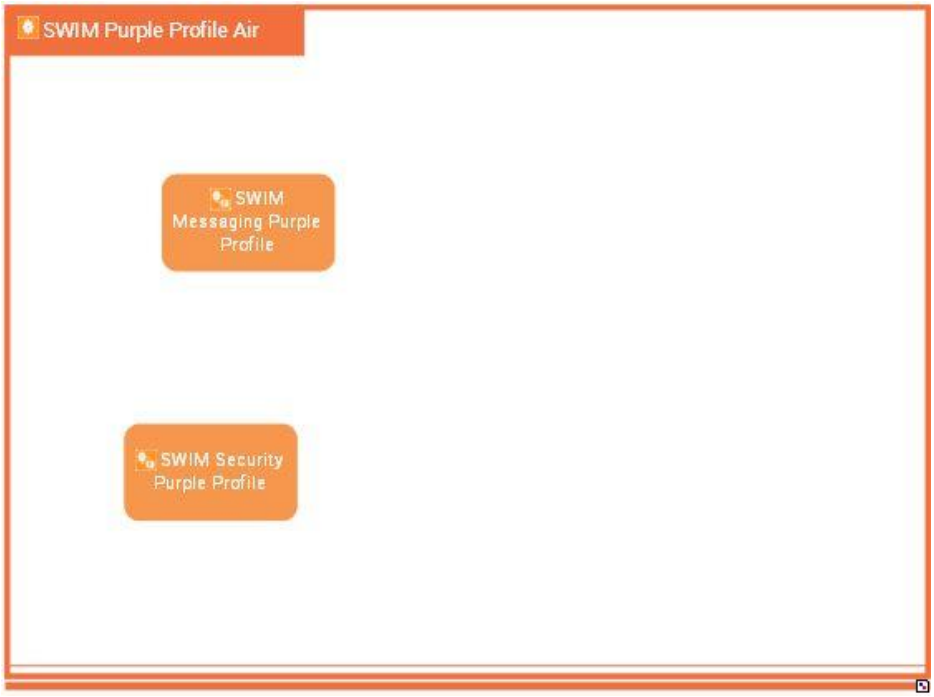


Figure 5: Artifact Structure Diagram - SWIM Purple Profile Air

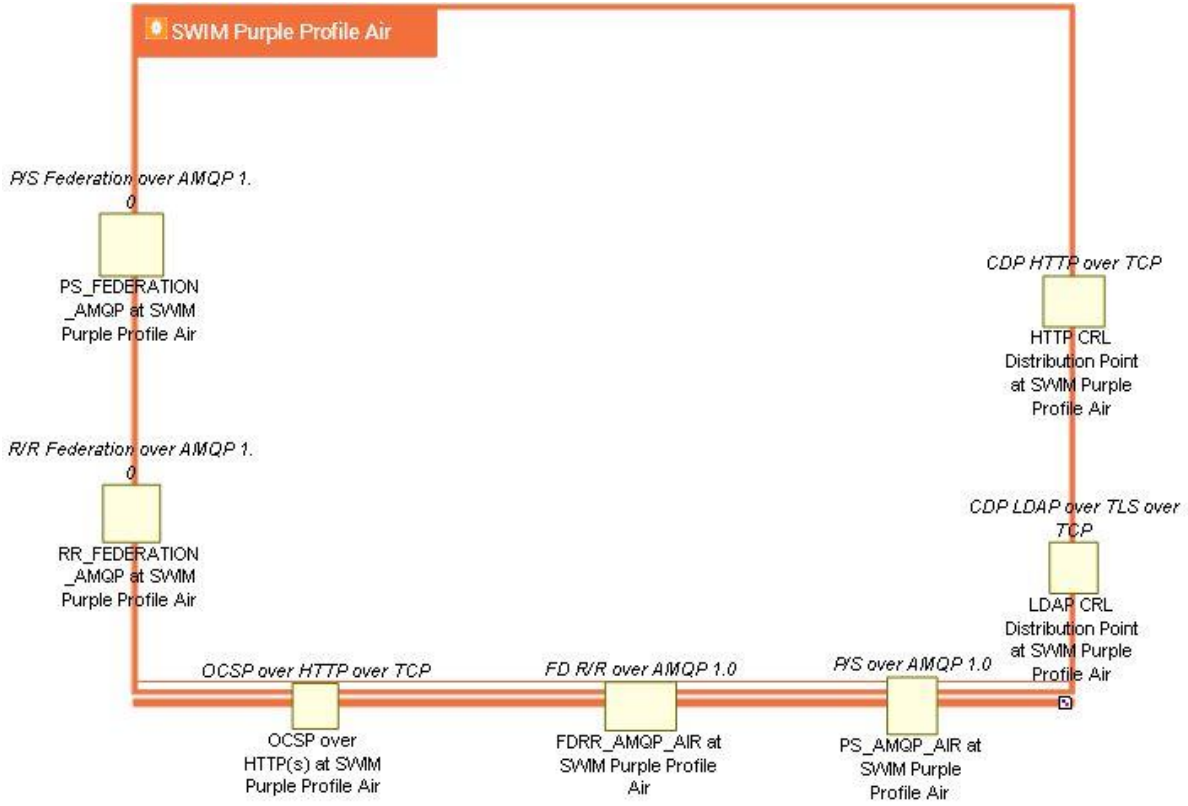


Figure 6: Artifact Assembly Diagram - SWIM Purple Profile Air

4.1.1 Resource Connectivity Model

The following NSV-1 diagrams represent the high-level interactions among the involved Capability Configurations. According to EATMA, the SWIM Purple Profile Air Technical System is part of the Civil Aircraft Capability Configuration. The exchange of weather information is depicted in Figure 7 and the exchange of aeronautical information is depicted in Figure 8. In both diagrams, the Communication Infrastructure (Capability Configuration) has been neglected in order to provide a clear view.

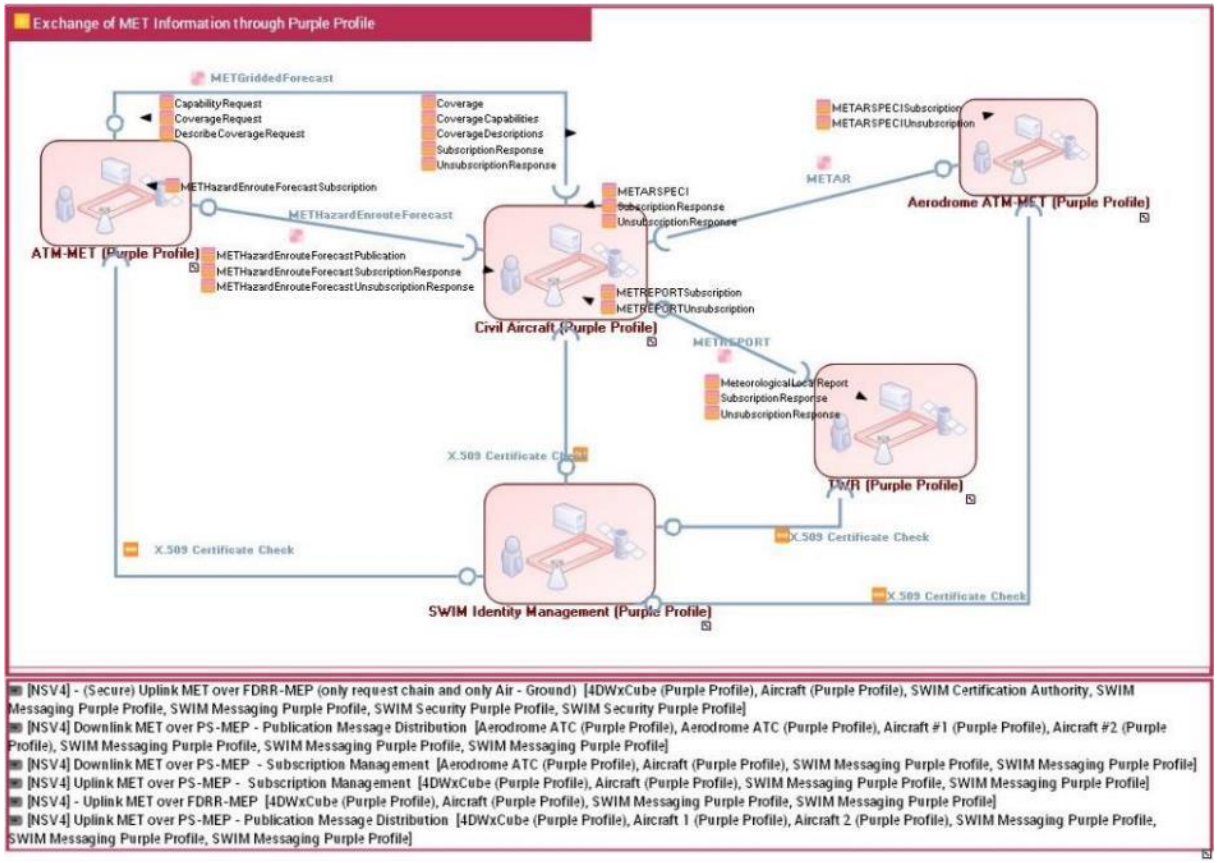


Figure 7: NSV-1 [Context] Exchange of MET Information through Purple Profile

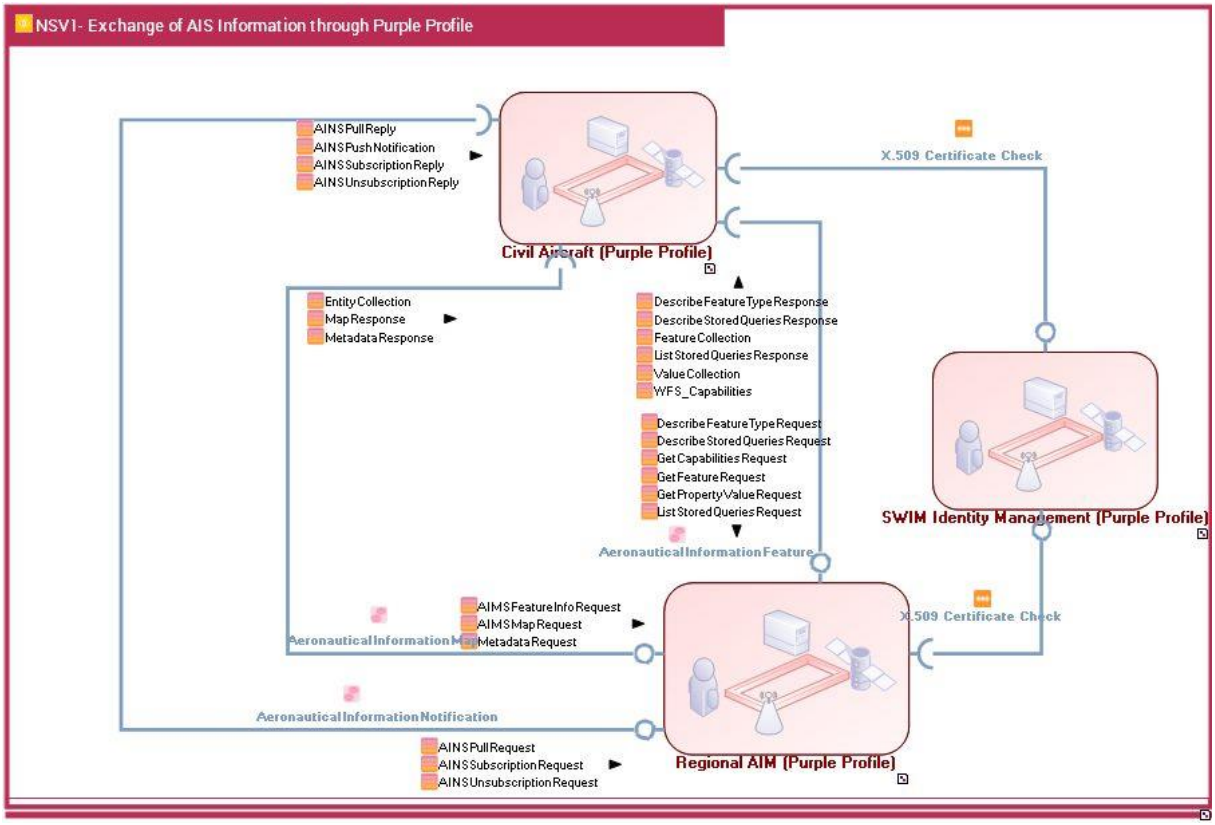


Figure 8: NSV-1 [Context] Exchange of AIS Information through Purple Profile

4.1.2 Resource Orchestration view

The diagrams within this section represent the interactions of the main FBs involved. There are five NSV-4 diagrams depicted to describe three out of six use cases since the other four are considered symmetrical and do not add any extra value to this section (refer to technical use cases described in §3.1.1.2). These diagrams have been derived from the functional and technical views described in §4.2.1 and §4.2.2.

The overall Purple Profile architecture is composed by following layers:

- Aircraft side application layer (SWIM service consumer/provider roles):
  - This layer is allocated to specific aircraft FBs/technical systems belonging to the Civil Aircraft CC.
- Aircraft/Airborne Communication network layer.
- Aircraft SWIM-TI layer (Aircraft Purple Profile SWIM Node):
  - This layer is allocated to aircraft side SWIM Purple Profile Technical System.
- Air/Ground Communication network layer.
- Ground SWIM-TI layer (federated with aircraft SWIM-TI layer, Ground Purple Profile SWIM Node):
  - This layer is allocated to ground side SWIM Purple Profile Technical System.
  - Different options exists in terms of CCs operating this technical system (§4.2.3). Provided diagrams are based on one possible option (ground side SWIM Purple Profile Technical System belongs to Civil AU Operation Centre CC)
- Ground/Ground Communication network layer.
- Ground SWIM-TI layer SWIM service consumer/provider side:
  - This layer is allocated to the CCs to which the ground technical system providing/consuming the service belongs to (e.g. ATM-MET CC, Regional AIM CC, etc.).
- Ground side application layer (SWIM service consumer/provider roles):
  - This layer is allocated to the CCs to which the ground technical system providing/consuming the service belongs to (e.g. ATM-MET CC, AIM (External) CC, etc.).

[NSV-4] Uplink MET over PS-MEP

This functional view depicts uplink of MET information in accordance with the PJ.17-01 reference technical use case PPUC-02 (Table 4~~Table 4~~). As described in the §4.2.2.2.1.2, information exchange based on Publish/Subscribe MEPs are based on four functions:

1. Subscription Management which deals with the life cycle of the interest that a subscriber expresses to be informed about particular publications or not.
2. Publication Registration Management which deals with the life cycle of the interest that a publisher expresses to perform particular publications
3. Message Distribution which deals with the delivery of the messages that contain the publications from the publisher to the publication consumers (PSPUSH-MEP and PSPULL-MEP).
4. Administration which deals with the management aspects such as configuration and monitoring.

Provided NSV4 views address both 1 (Figure 9~~Figure 9~~) and 3 (Figure 10~~Figure 10~~). Subscription Management is based on the FDRR-MEP where:

- Requestor = subscriber
- Responder = subscription handler.
- Request and response messages are in accordance with Purple Profile defined AMQP annotated message and Subscription Management XSD.
    - (Logical) METARSPECISubscription and METARSPECISubscriptionResponse data elements have to be properly instantiated on PP Subscription Management.

(Logical) METARSPECI data element have to be properly instantiated in accordance with PP AMQP annotated message.

In this TS several technical and deployment options are allowed. Provided NSV4 diagrams are based on the following design/deployment decisions:

- Subscription handler responsible for accepting the requests is deployed on the Purple Profile Ground.
- Ground side message topic used to publish publication messages is deployed on the Purple Profile Ground.

Security functionality has not been described due complexity to represent together with messaging functionality.

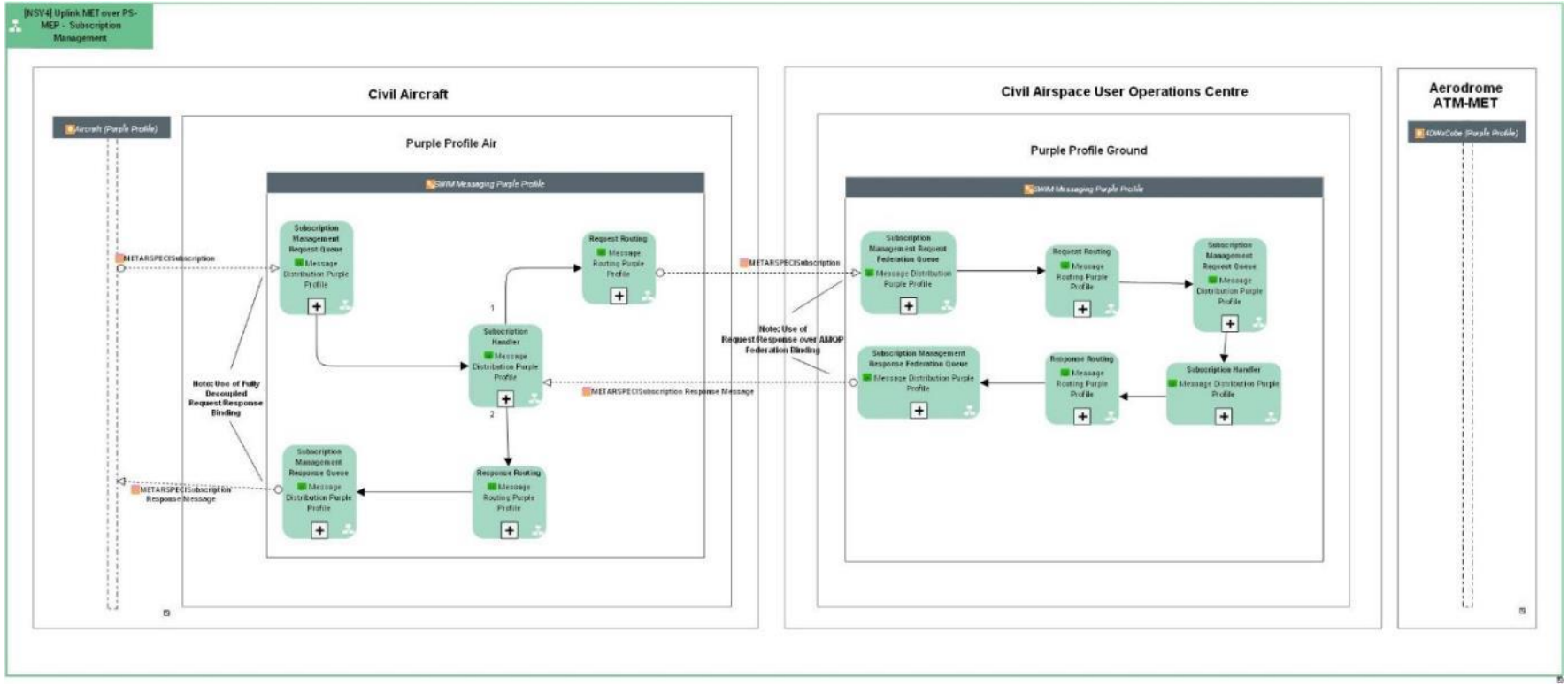


Figure 9: [NSV-4] Uplink MET over PS-MEP- Subscription Management

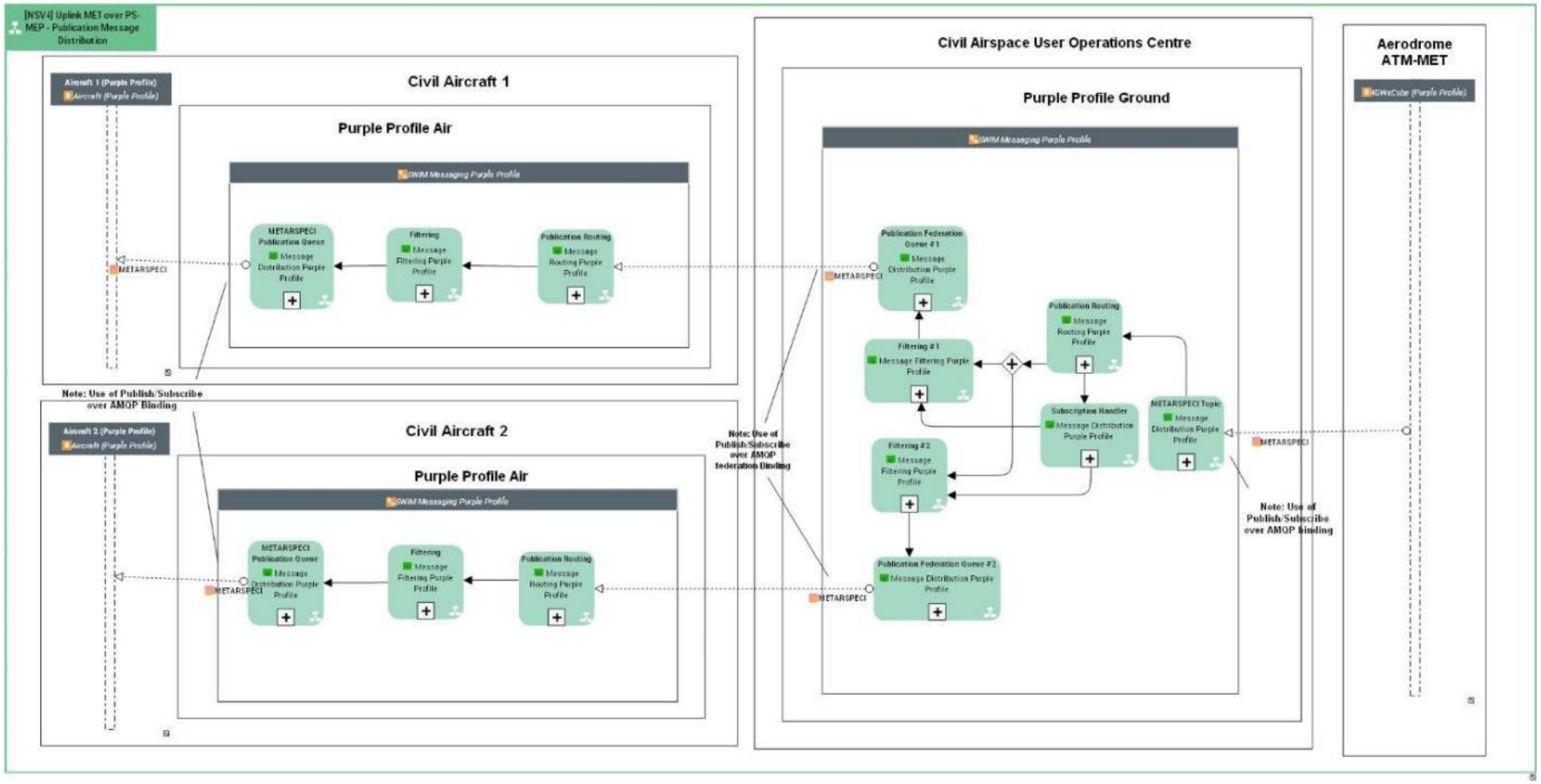


Figure 10: [NSV-4] Uplink MET over PS-MEP – Publication Message Distribution

[NSV-4] Downlink MET over PS MEP

This functional view depicts downlink of MET information in accordance with the PJ.17-01 reference technical use case PPUC-04 (Table 4~~Table 4~~).

As for Uplink MET over PS-MEP, provided NSV4 views address subscription management (Figure 11~~Figure 11~~) and message distribution (Figure 12~~Figure 12~~). Subscription Management is based on the FDRR-MEP where:

- Requestor = subscriber
- Responder = subscription handler.
- Request and response messages are in accordance with Purple Profile defined AMQP annotated message and Subscription Management XSD.
    - (Logical) METREPORTSubscription and METREPORT Subscription Response data elements have to be properly instantiated on PP Subscription Management.

(Logical) METREPORT data element have to be properly instantiated in accordance with PP AMQP annotated message.

In this TS several technical and deployment options are allowed. Provided NSV4 diagrams are based on the following design/deployment decisions:

- Subscription handler responsible for accepting the requests is deployed on the Purple Profile Ground.
- Ground side message topic used to publish publication messages is deployed on the Purple Profile Ground.

Security functionality has not been described due complexity to represent together with messaging functionality.

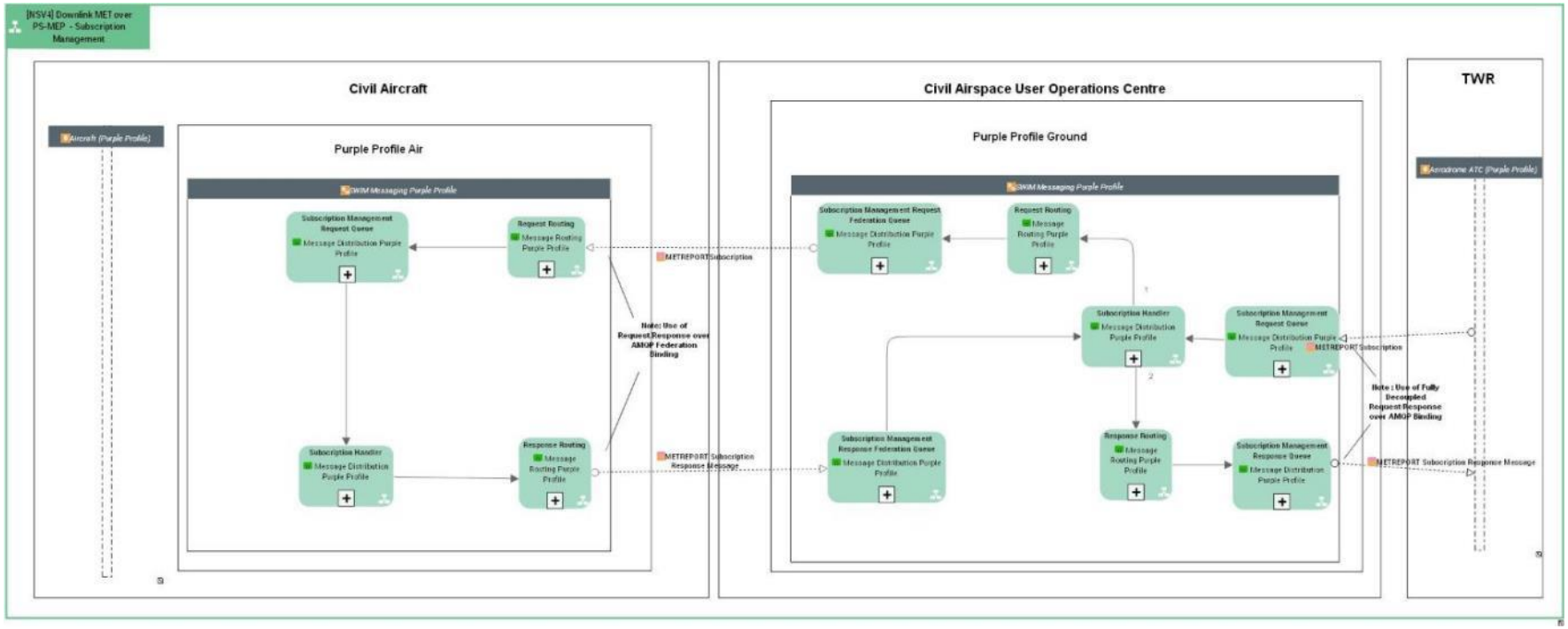


Figure 11: [NSV4] Downlink MET over PS-MEP – Subscription Management

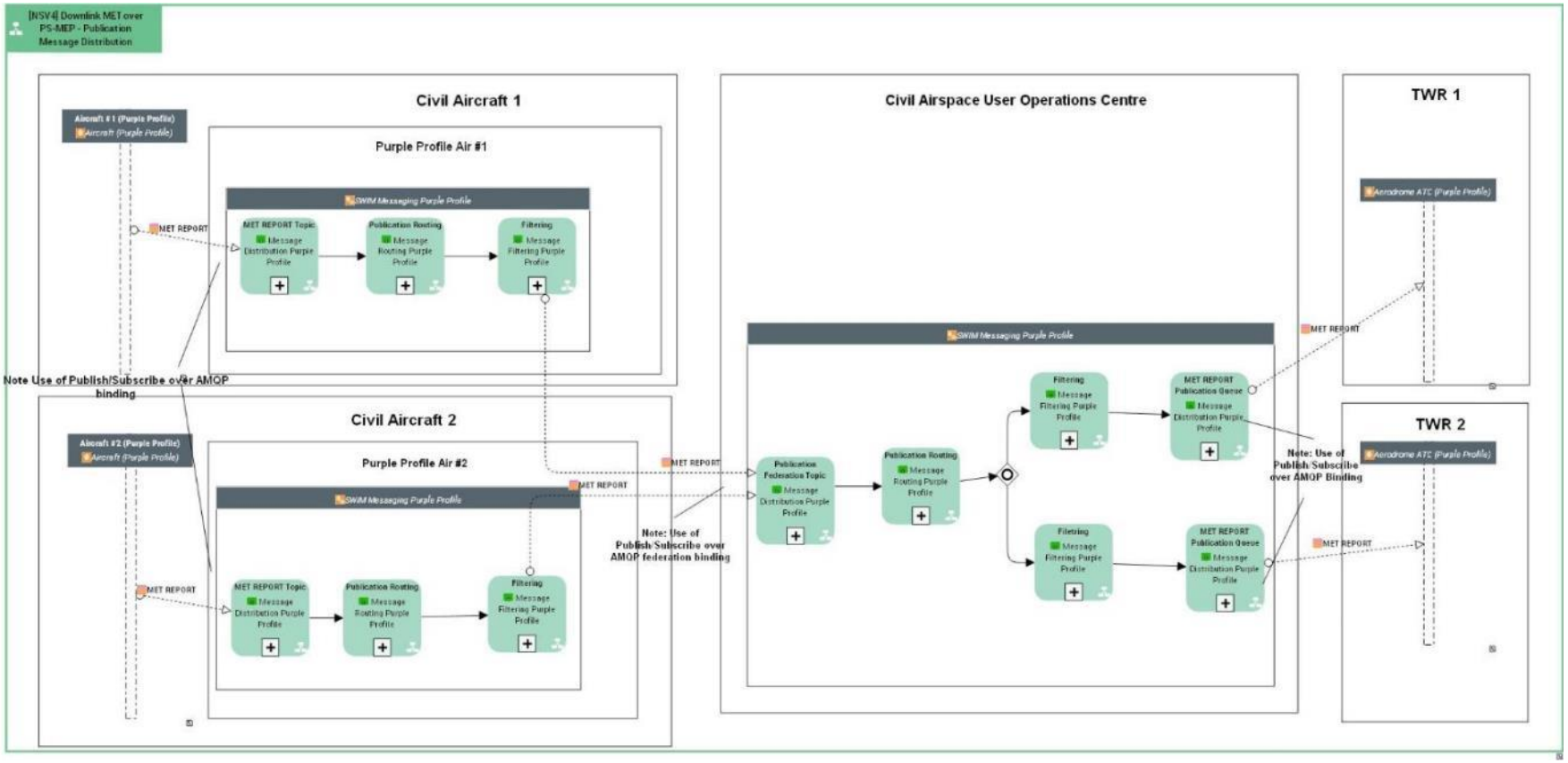


Figure 12: [NSV4] Downlink MET over PS-MEP – Publication Message Distribution

[NSV4] Uplink MET over FDRR-MEP

This functional view depicts uplink of MET information in accordance with the PJ.17-01 reference technical use case PPUC-01a (Table 4~~Table 4~~).

As described in the §4.2.2.2.1.1, information exchange based on Request/Response MEPs are based on following functions:

1. Message Distribution which deals with the delivery of the request and response messages.
2. Administration which deals with the management aspects such as configuration and monitoring.

Provided NSV4 view addresses only message distribution function (Figure 13~~Figure 13~~). Due non existing MET service with this MEP, no service has been chosen for this view. Instead Request and Response empty data elements have been instantiated for context purpose. Of course, it would be possible that the response concerns METARSPECI data element introduced above.

In this TS several technical and deployment options are allowed. Provided NSV4 diagrams are based on the following design/deployment decisions:

- Request and response message queues deployed on the Purple Profile Ground.

Security functionality has not been described due complexity to represent together with messaging functionality.



Figure 13: [NSV4] Uplink MET over FDRR-MEP

[NSV4] Secure Uplink MET over FDRR-MEP

Due the complexity to represent together messaging and security aspects, all the NSV4 views provided above do not describe any security functionality. Although in the technical viewpoint all the security controls are described, for completeness two examples of authentication and authorization enforcement are provided. As anticipated in §4.1, the diagrams are an attempt to put together functional and technical aspects using EATMA meta-model: actual reference design is provided in the technical viewpoint description (§4.2.2).

In particular, starting from the NSV4 view for Uplink MET over FDRR-MEP (Figure 13), authentication and authorization for the "request chain" are described in Figure 14 and Figure 15. The "response chain" (Figure 13) is not depicted because it is very similar: the only difference is the concerned messaging resources (response queues).

- In Figure 14, Aircraft and Ground Purple Profile enabled applications authentication and authorization are described. On the air side, the Aircraft (Purple Profile) has to be authenticated and then authorized to write to the "ATM-MET Request Queue" (Figure 13 and Figure 14). The authentication is based on X.509v3 certificates and certificate revocation status check is enforced using local CRL. The same applies on the ground side, where the 4DWxCube (Purple Profile) has to be authenticated and then authorized to read from the "ATM-MET Request Queue" (Figure 13 and Figure 14). The authentication is based on X.509v3 certificates and, although also CRL based option is allowed on the ground, certificate revocation status check is enforced via OCSP service.
- In Figure 15, Air SWIM Node authentication and authorization is described: the Purple Profile Air technical system has to be authenticated and authorized to write to the "Request Federation Queue" (Figure 13 and Figure 15). The diagram shows mutual authentication with certificate revocation status check based on local CRL on the air side, and via OCSP service on the ground side.

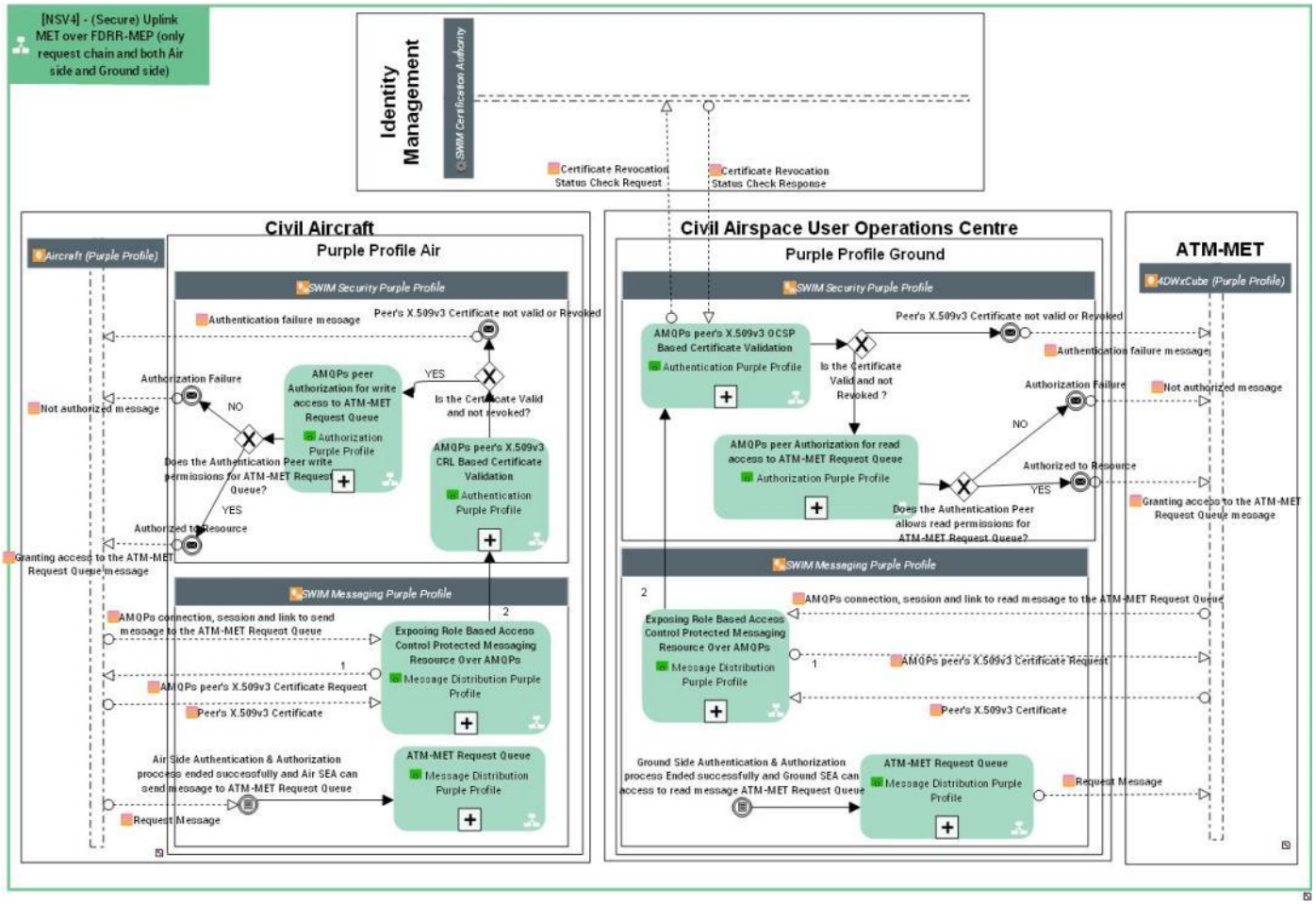


Figure 14: [NSV4] Uplink MET over FDRR-MEP – Aircraft and Ground Purple Profile enabled applications authentication and authorization

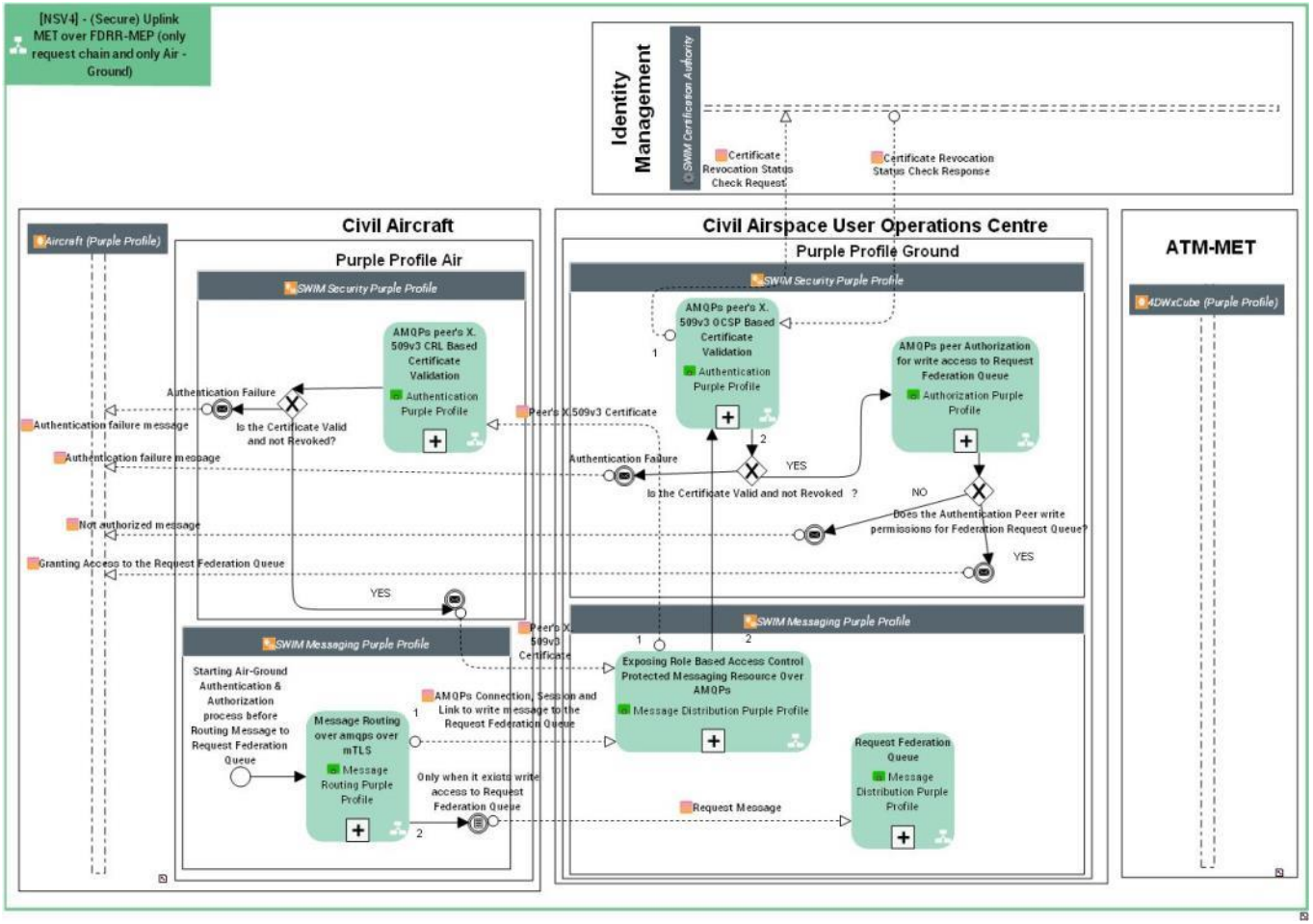


Figure 15: [NSV4] Uplink MET over FDRR-MEP – Air SWIM Node authentication and authorization

4.1.3 Infrastructure connectivity model

Figures in this section show the supporting infrastructure at a Capability Configuration level in order to detail at physical level the communication technologies used in the interactions between CCs and between technical systems.

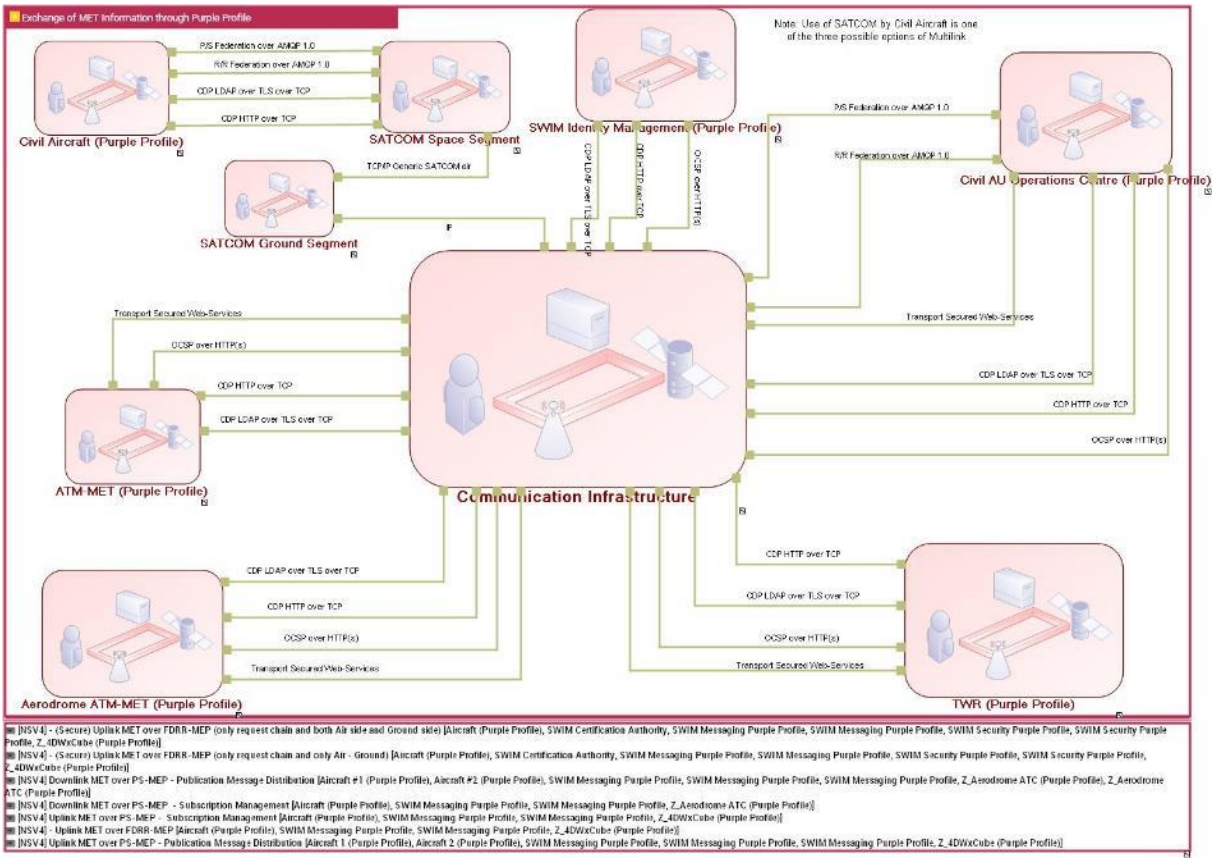


Figure 16: MET NSV-2 Infrastructure Connectivity Model

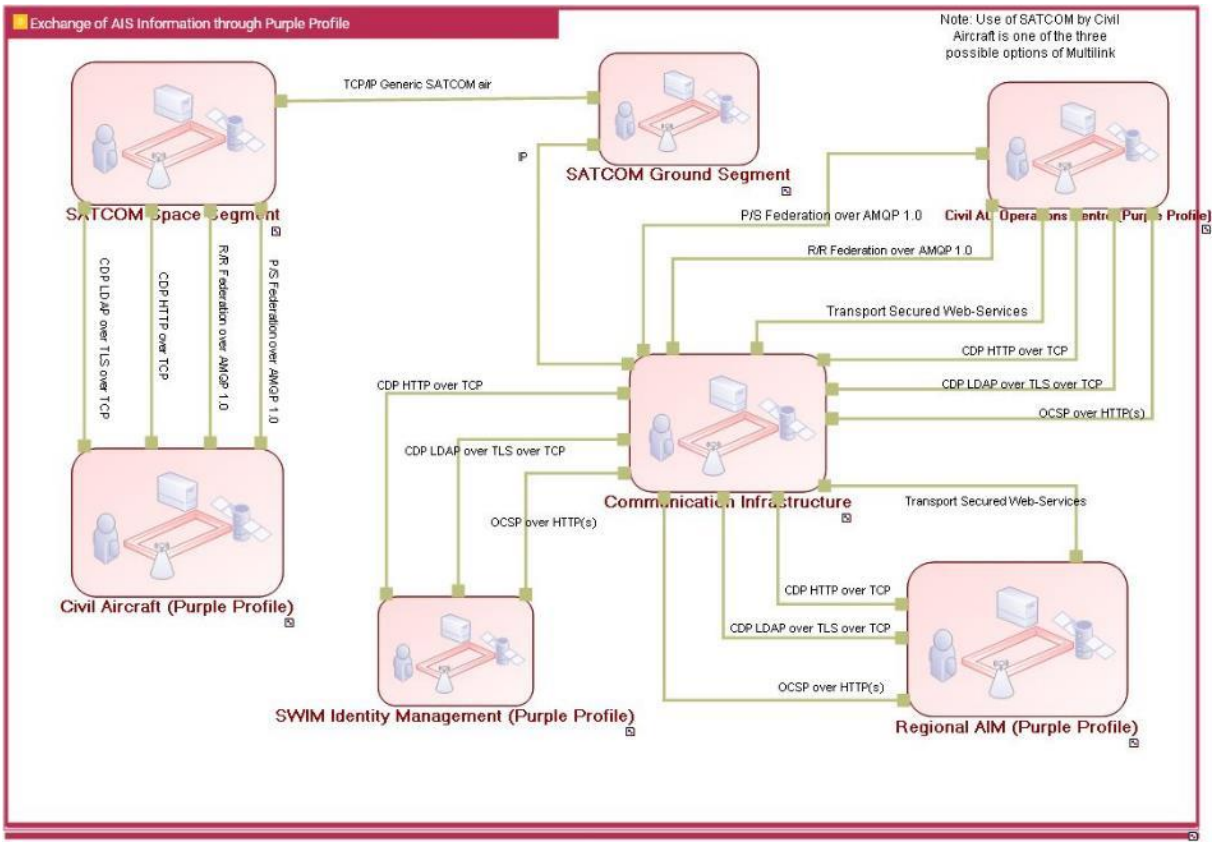


Figure 17: AIS NSV-2 Infrastructure Connectivity Model

In order to detail the physical interactions of the SWIM Purple Profile technical system within a Capability Configuration, a diagram of the Civil Aircraft CC is detailed in Figure 18 as an example.

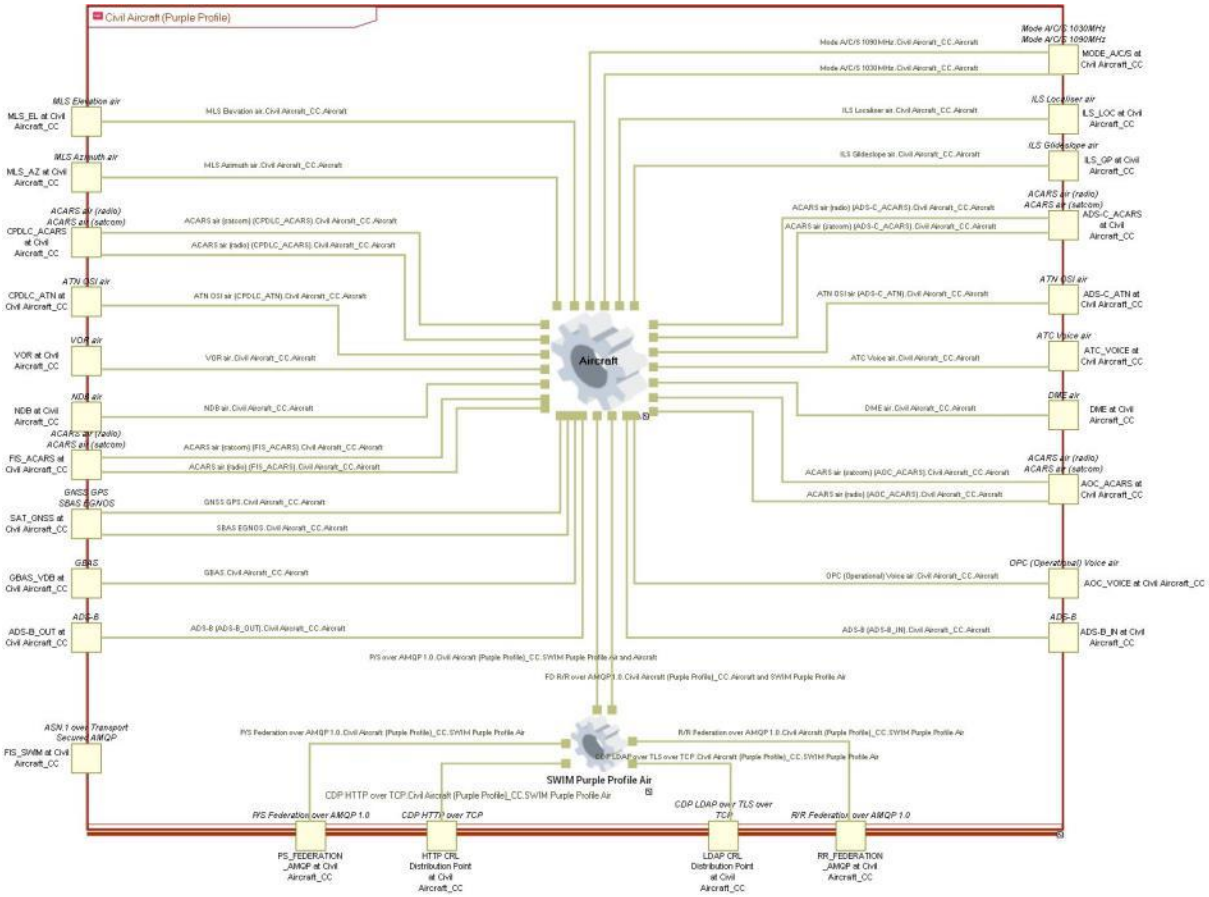


Figure 18: Infrastructure connectivity model within the Civil Aircraft CC

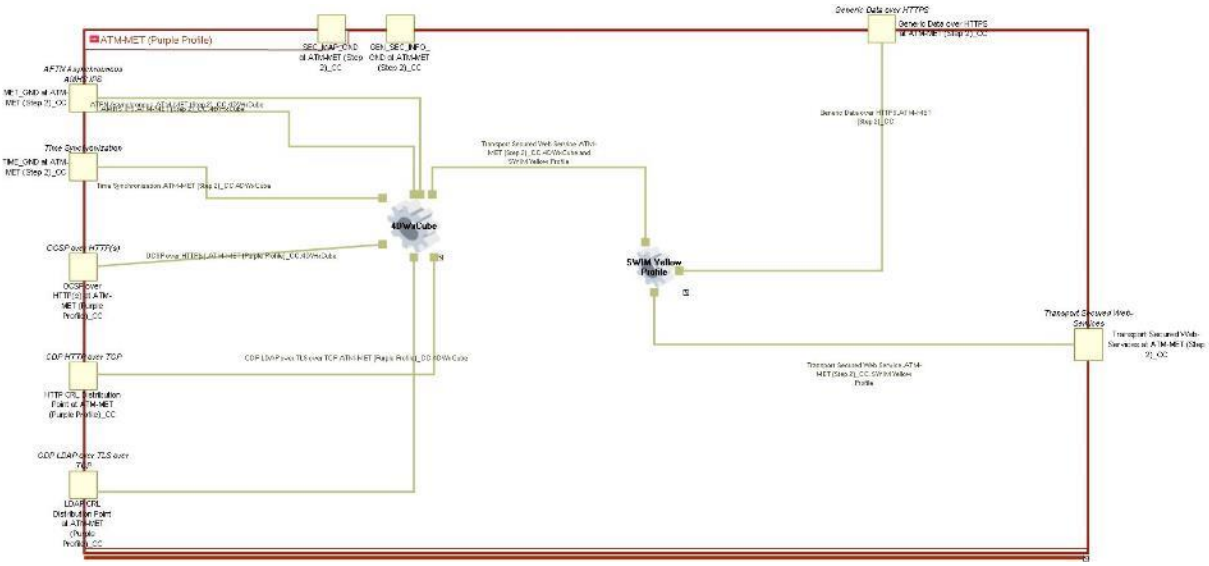


Figure 19: Infrastructure connectivity model within the ATM-MET CC

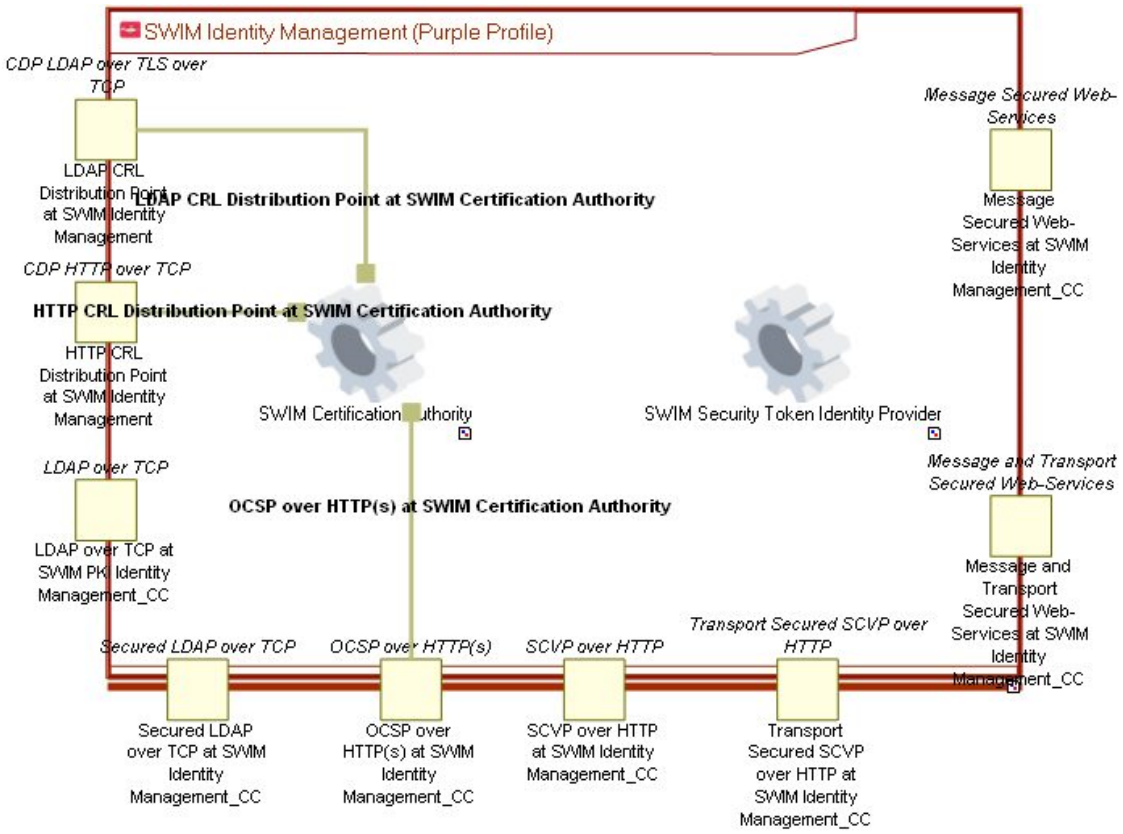


Figure 20: Infrastructure connectivity model within the SWIM Identity Management CC

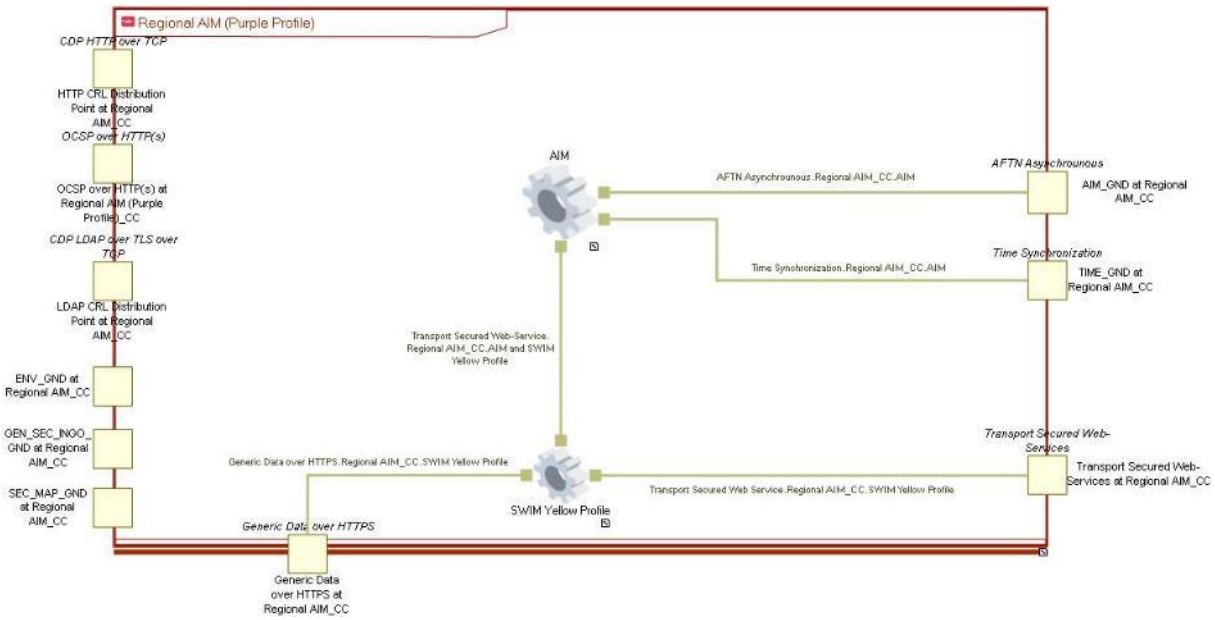


Figure 21: Infrastructure connectivity model within the Regional AIM CC

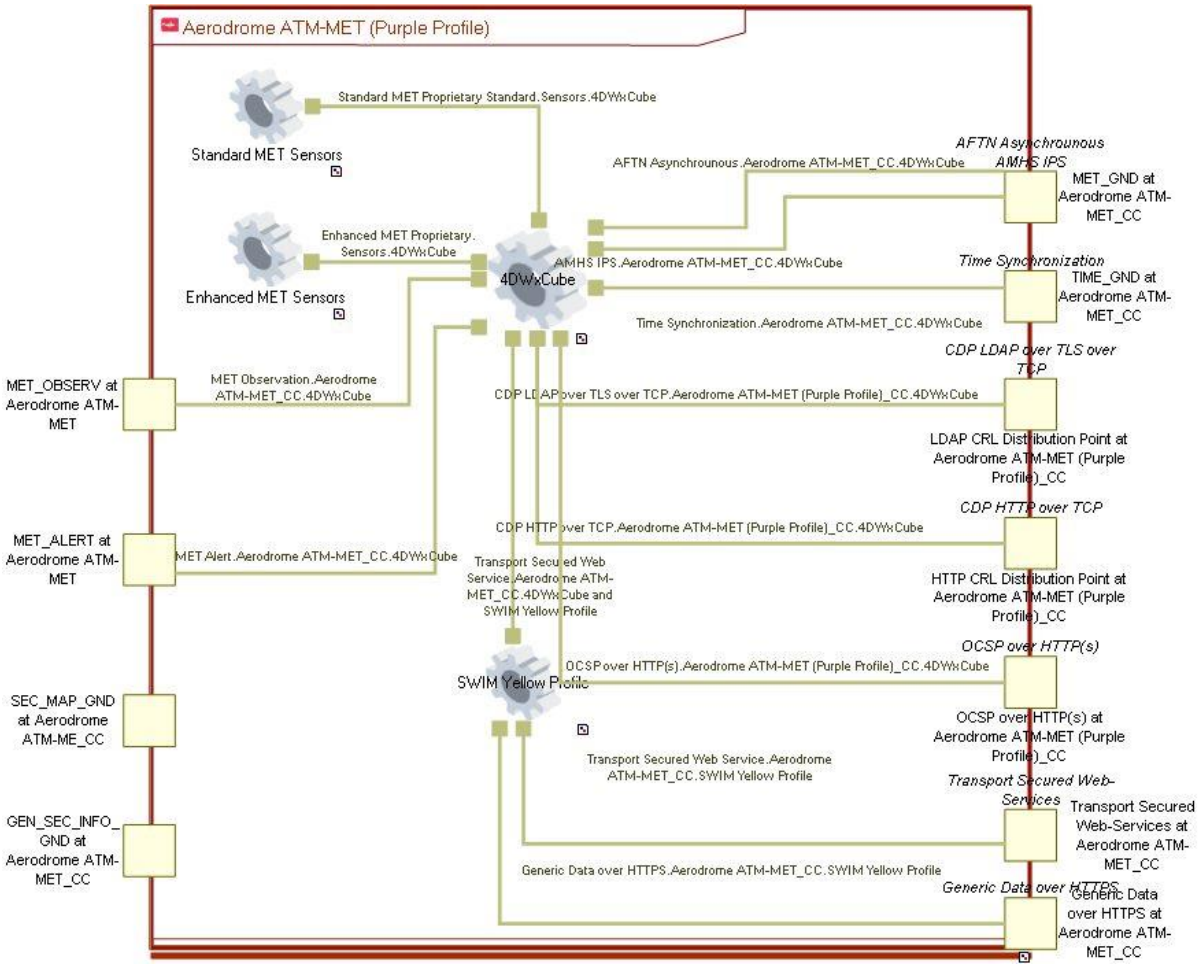


Figure 22: Infrastructure connectivity model within the Aerodrome ATM-MET CC

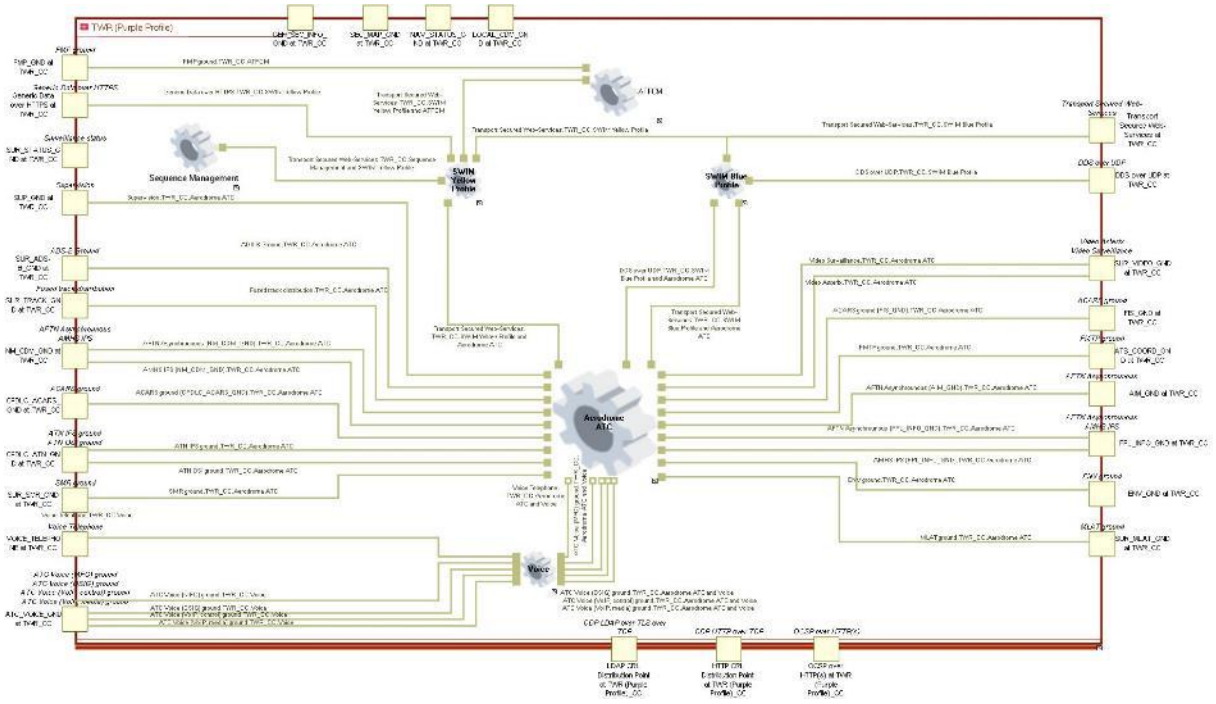


Figure 23: Infrastructure connectivity model within the TWR CC

4.1.4 Service view

In accordance with §3.1, the PJ.17-01 technological solution contributes to one of the SESAR Key Features and, in the context of this solution, the enabling SWIM-TI functions for Air-Ground SWIM are designed, specified and validated (technical validation). The SWIM-TI contributes to the solution aspect of the services and the SWIM service identification and design is out of scope of this solution. Both Aircraft and Ground SWIM applications are based on service oriented architecture (SOA) models and technologies and the Air–Ground SWIM has to consider constraints (QoS, security, or cost) of radio links and associated protocols. It's inefficient or even impossible for the Aircraft SWIM applications to directly interface with Ground SWIM services that do not consider such constraints.

This solution provides the enabling technical infrastructure and service interface binding's options: it is up to the SWIM service architect to select (service technical design) the appropriate interface binding(s).

The diagrams included in this section represent the logical view of the EATMA architectural functional decomposition of involved actors. Resource Architecture Structure diagrams in the context of a Capability Configuration depict the logical interaction between owned systems and owned service interface (use) elements, through which is described which SWIM service definitions or resource interactions are consumed or provided in the depicted Capability Configuration. Artifact Assembly Diagrams in the context of a Technical system represent through its service interface (use) owned elements which service interface definitions are able to be consumed and provided. In addition, it represents the system ports through which a given service interface is realised.

The SWIM Purple Profile Air and Ground technical systems are not the providers or consumers of the SWIM services, and this is why no service interface (use) request points are included in the architecture of both technical systems. Instead those logical ports are modelled in the logical

provider and/or consumer of the SWIM services as depicted in the next diagrams for ‘Aircraft’, ‘4DwxCube’, and ‘Aerodrome ATC’.

Taking into account that SWIM services used as examples in the architecture of this solution (e.g. ‘METREPORT’, ‘METAR’, ‘METGriddedForecast’) are all based on the Publish/Subscribe MEP, the service interface (use) elements are only connected to the system ports related to the bindings defined for that MEP. Related system ports implementing Request/Response MEP bindings have no connections to service interface request points.

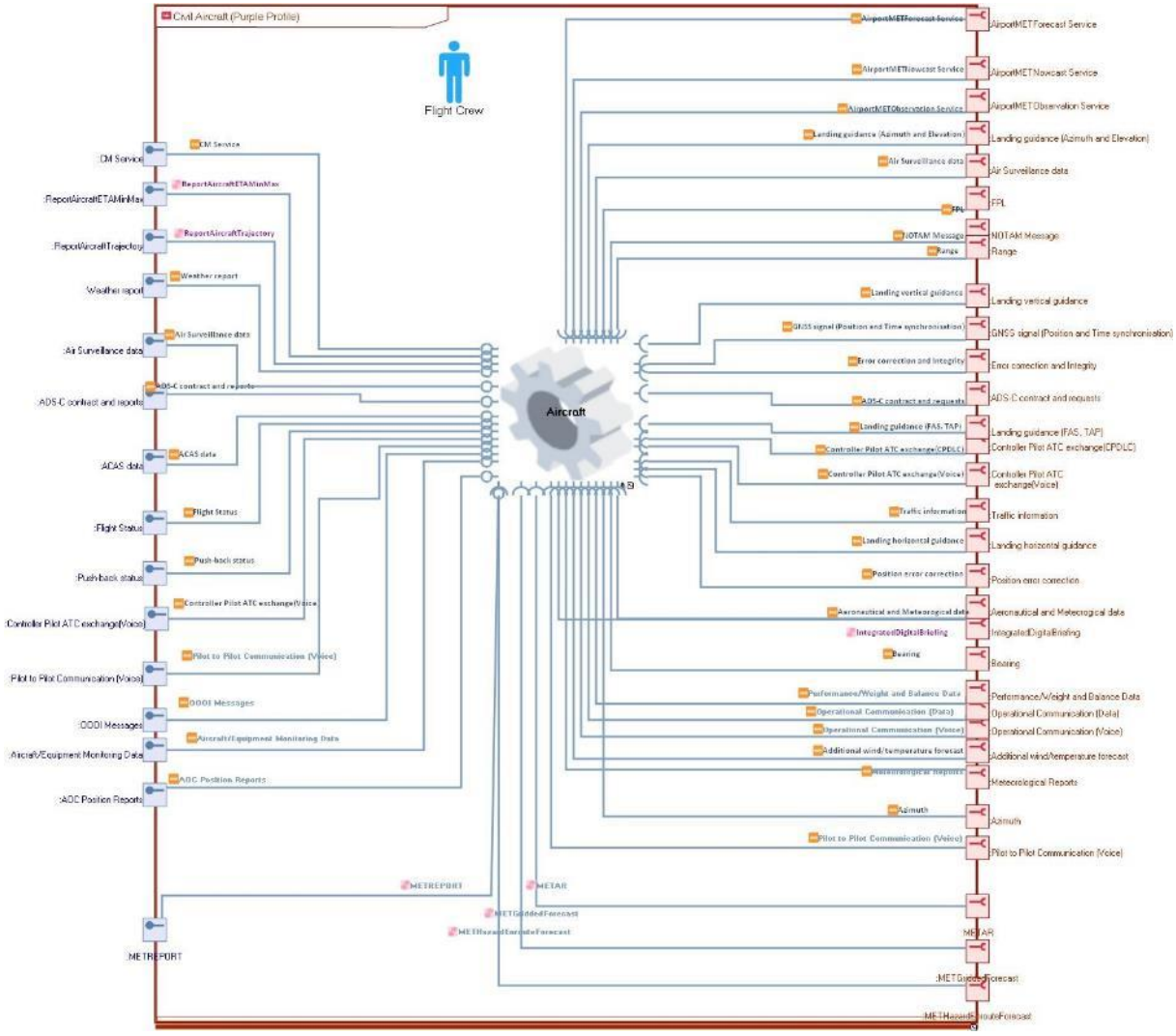


Figure 24: Resource Architecture Structure Diagram within the Civil Aircraft CC

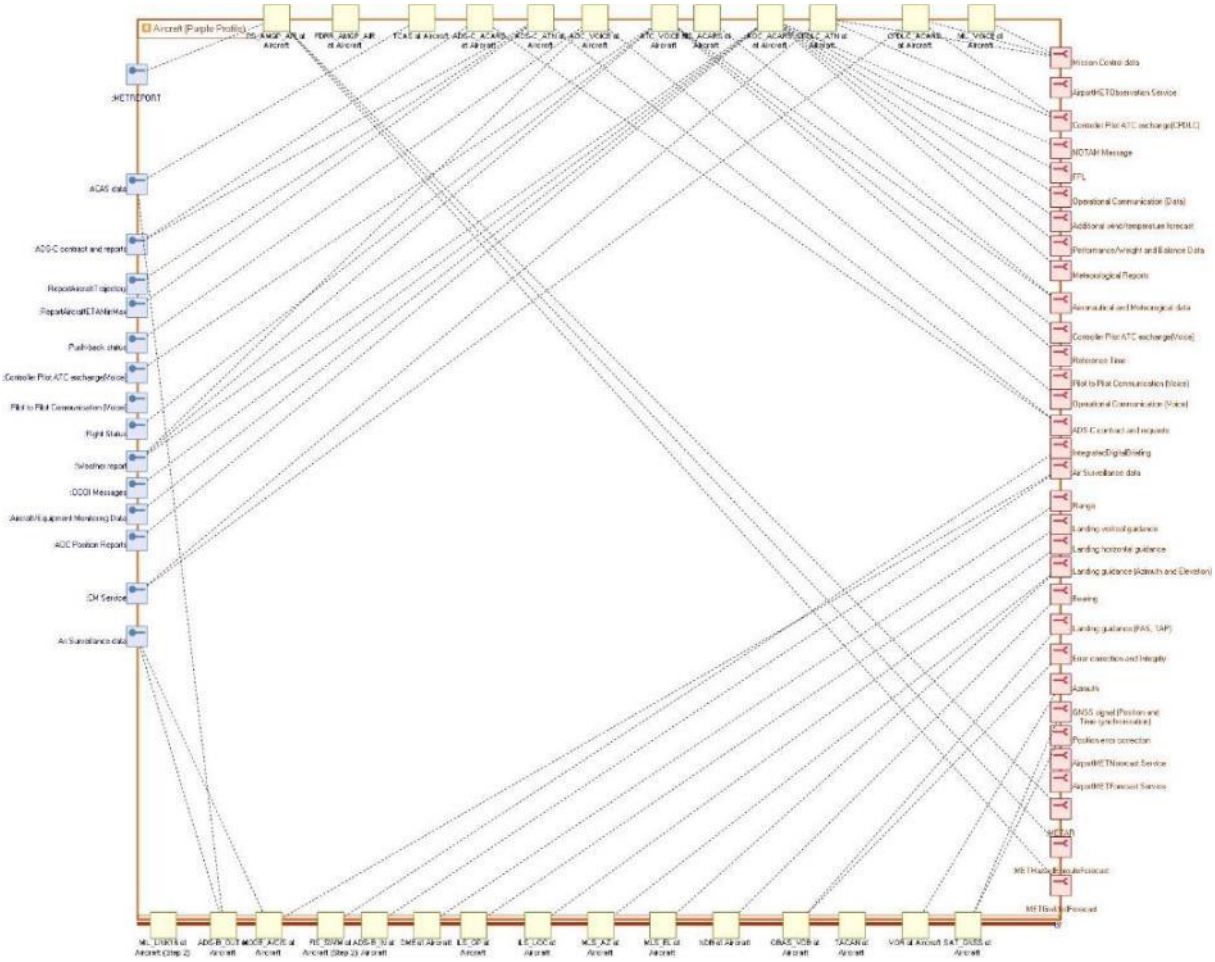


Figure 25: Artifact Assembly Diagram within the Aircraft Technical System

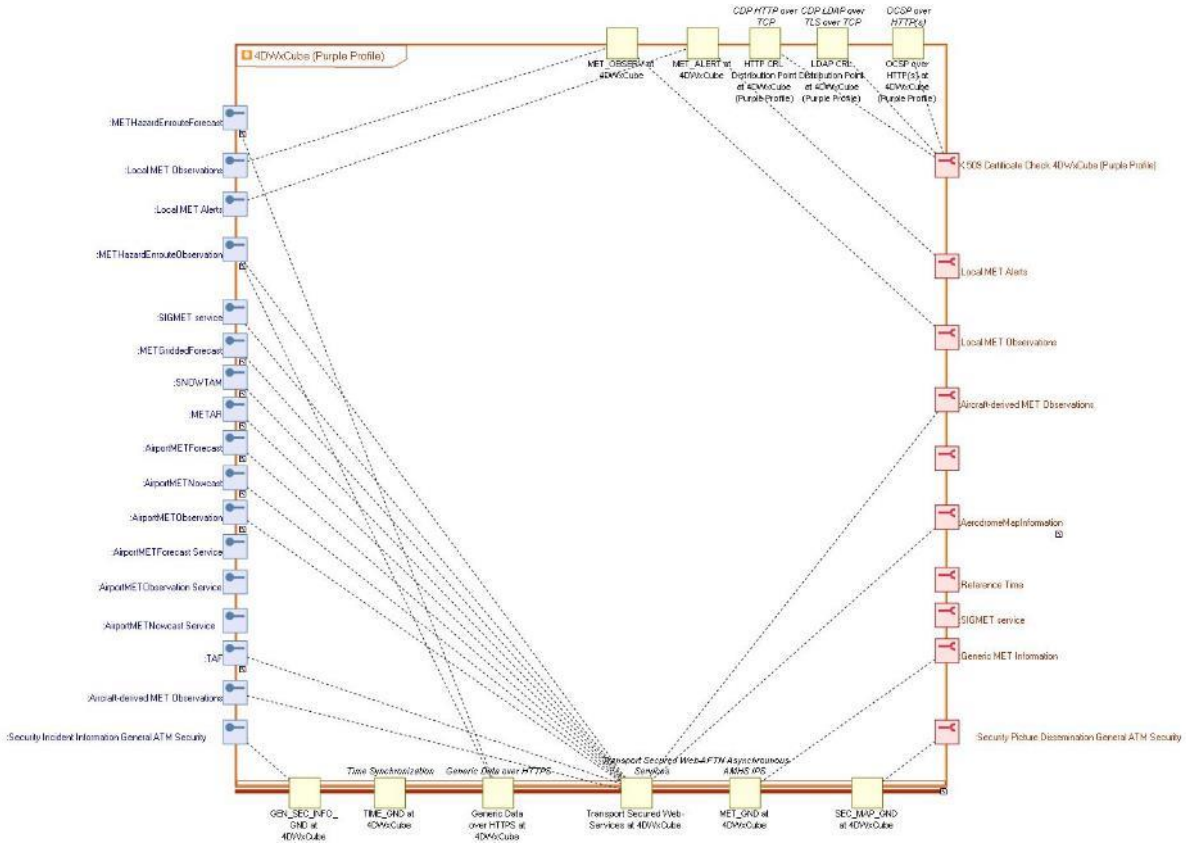


Figure 26: Artifact Assembly Diagram within the 4DWxCube Technical System

In order to design Bindings elements in EATMA, it has been defined a Binding (definition) element per Binding requirement. In addition, in order to represent that a Binding *Binds* a given service interface to a system port, in an agnostic way to the Binding (definition) elements, a new element has been created: the 'Binding *(Use)*'. The table below represents the modelling of the mentioned elements with the related service interfaces and system ports elements.

Binding (Use element)	Binding (Definition Element)	Service Interface (Use element)	System Port
P/S over AMQP 1.0 Binding.METREPORTInterface	P/S over AMQP 1.0 Binding	METREPORT.Aircraft	PS_AMQP_AIR at SWIM Purple Profile Air
P/S over AMQP 1.0 Binding.~METREPORTInterface		METREPORT.Aerodrome ATC	PS_AMQP_Ground at SWIM Purple Profile Ground
P/S over AMQP 1.0 Binding.METARInterface		METAR.4DWxCube	PS_AMQP_Ground at SWIM Purple Profile Ground

P/S over AMQP 1.0 Binding.~METARInterface		METAR.Aircraft	PS_AMQP_AIR at SWIM Purple Profile Air
P/S over AMQP 1.0 Binding.METHazardEnrouteForecast		METHazardEnrouteForecast.4DWxCube	PS_AMQP_Ground at SWIM Purple Profile Ground
P/S over AMQP 1.0 Binding.~METHazardEnrouteForecast		METHazardEnrouteForecast.Aircraft	PS_AMQP_AIR at SWIM Purple Profile Air
P/S over AMQP 1.0 Binding.METGriddedForecastInterface		METGriddedForecast.4DWxCube	PS_AMQP_Ground at SWIM Purple Profile Ground
P/S over AMQP 1.0 Binding.~METGriddedForecastInterface		METGriddedForecast.Aircraft	PS_AMQP_AIR at SWIM Purple Profile Air

Table 9: Bindings (Use) Elements with related service interfaces (use elements) and system ports

4.2 Architectural Views

In order to describe the Purple Profile architecture in a structured manner, the ISO/IEC/IEEE 42010:2011 standard is adopted in this TS. In particular different actors[4] (i.e. "stakeholders" in ISO/IEC/IEEE 42010:2011), concerns, architecture viewpoints and architecture views are identified and described. The viewpoints are based on the "what", "how", "how good" and "where" SWIM-TI aspects described in the introduction of §4.

In this section the architectural views concerning the Purple Profiles viewpoints introduced above are described. In particular:

- **The Functional viewpoint** is described via the Purple Profile Functional view §4.2.1 and concerning requirements in §4.3.1.
- **The Technical Viewpoint** is described via the Purple Profile Technical view in §4.2.2 and concerning requirements in §4.3.2-§4.3.7.
- **Deployment Viewpoint** is described via the Purple Profile Deployment view in §4.2.3.

Purple Profile Functional Viewpoint

The Purple Profile functional viewpoint addresses the "what" without dealing with the "where" or "how" aspects of the SWIM-TI. It mainly addresses the concern about what the Purple Profile technical systems shall/should/could do. The concern is described in terms of identification of applicable SWIM-TI functions from EATMA and functional requirements.

In particular, the SWIM-TI functional decomposition from EATMA is assessed and applicable functions are selected taking into account the Purple Profile SWIM Profile SPA (SWIM Profile Assertion) [Appendix A] and applicable EN.

From the highest level of abstraction, the Purple Profile technical systems is considered as a single entity providing functions with the purpose of ensuring technical interoperability between Purple Profile enabled technical systems providing/consuming Purple Profile enabled SWIM services.

The functional viewpoint is described in the Purple Profile Functional view in §4.2.1 and it is based on the messaging characterization in Appendix B. Requirements concerning this view are provided in §4.3.1. In order to allow this view to persist and remain valid across technology changes, it is expected to be independent of and totally silent about specific technology.

Following tables provide the characterization of this viewpoint in terms of concerns and actors.

Concern ID	Concern	Actors
PPArchC01	The purpose of the Purple Profile technical systems	Primarily PArchA01 and PArchA02.

[4] The term actor is used to avoid confusion with (ATM) "Stakeholder" as defined in EATMA.

PPArchC02	The functional level suitability of the Purple Profile technical systems architecture for enabling Air-Ground advisory information sharing via SWIM Purple Profile enabled SWIM services.	Primarily PArchA03 and PArchA04.

Table 10: List of Concerns framed by the functional viewpoint

Actor ID	Actor	Concerns
PPArchA01	Purple Profile technical systems user	Primarily PPArchC01 but concerned also of PPArchC02.
PPArchA02	Purple Profile technical systems developer	Primarily PPArchC01 but concerned also of PPArchC02.
PPArchA03	Purple Profile enabled SWIM service architect	Primarily PPArchC02 but concerned also of PPArchC01.
PPArchA04	EATMA architect	Primarily PPArchC02 but concerned also of PPArchC01.

Table 11: List of Actors interested to the functional viewpoint

Purple Profile Technical Viewpoint

The technical viewpoint complements and specializes the “what” aspect addressing the “how” and “how good” but without dealing with the “where” aspect of the SWIM-TI. It provides the technical view according to technical architecture and technical interoperability needs (“how”) and SWIM-TI’s NFRs (“how good”). It mainly addresses the concern about how to realize the sub-set of functions according to interoperability needs assessment. The concern is described in terms technical architecture definition, SWIM interface binding requirements, technical requirements and non-functional requirements.

The component that can provide/realize/deploy the functions of the functional view is the SWIM-TI Node: a SWIM-TI Node is an autonomous point of presence in the Distributed System (of Systems) that interacts with other SWIM-TI Nodes in the Distributed System (of Systems). The point of presence makes a set of functionality via one SWIM-TI Node available to any SWIM-TI Node or allows use of the functionality that is made available by a SWIM-TI Node via one or more SWIM-TI Nodes.

The autonomy of a SWIM-TI Node reflects the freedom (implementation choices such as but not limited to hardware/virtualisation, OS, high availability techniques and platform) and governance (such as but not limited to development process, running of operations and definition of policies).

The technical viewpoint is described in the Purple Profile Technical view in §4.2.2. Requirements concerning this view are provided in §4.3.2-§4.3.7.

Following tables provide the characterization of this viewpoint in terms of concerns and actors.

Concern ID	Concern	Actors
PPArchC03	The suitability of the Purple Profile technical systems	PPArchA01, PPArchA02,

Company General Use

	architecture for achieving its purposes.	PPArchA05, PPArchA03, PPArchA04
PPArchC04	Implementation and maintenance of the Purple Profile technical systems.	PPArchA02
PPArchC05	Technical validation of the Purple Profile technical systems realization.	PPArchA02, PPArchA05
PPArchC06	The technical level suitability of the Purple Profile technical systems architecture for enabling Air-Ground advisory information sharing via SWIM Purple Profile enabled SWIM services.	PPArchA01, PPArchA02, PPArchA05, PPArchA03, PPArchA04

Table 12: List of Concerns framed by the technical viewpoint

Actor ID	Actor	Concerns
PPArchA01	Purple Profile technical systems user	Primarily PPArchC03 but concerned also of PPArchC06.
PPArchA02	Purple Profile technical systems developer	Primarily PPArchC03, PPArchC04 and PPArchC06 but concerned also of PPArchC05.
PPArchA05	Purple Profile technical systems validation result analyst	Primarily PPArchC05 but concerned also of PPArchC03 and PPArchC06.
PPArchA03	Purple Profile enabled SWIM service architect	Primarily PPArchC06 but concerned also of PPArchC03.
PPArchA04	EATMA architect	Primarily PPArchC06 but concerned also of PPArchC03.

Table 13: List of Actors interested to the technical viewpoint

Purple Profile Deployment Viewpoint

The deployment viewpoint provides deployment options addressing the "where" in terms of architecture technical and integration options. It mainly addresses the concern about how to deploy the ("what" and "how" of) Purple Profile.

General recommendations/principles about the deployment options [51]:

- *Deployment options should not break interoperability*,
- *Deployment options should not be in contradiction with documented design decisions and principles*,
- *If any additional requirement is needed to support such deployment option it shall be identified and specified*.

This specification does not impose/restrict the deployment options. Furthermore, the list of deployment options is not supposed to be complete and exhaustive.

The deployment viewpoint is described in the Purple Profile Deployment view in §4.2.3.

Following tables provide the characterization of this viewpoint in terms of concerns and actors.

Concern ID	Concern	Actors
PPArchC07	A/C Airworthiness	Aeroplane operator
PPArchC08	A/C Continuous Airworthiness	Aeroplane operator
PPArchC09	Flight regularity (Aircraft dispatch)	Commercial Air Transport operator
PPArchC10	Configuration, deployment, testing and qualification of the Purple Profile technical systems in aeronautical operational environment	PPArchA07, PPArchA08

Table 14: List of Concerns framed by the deployment viewpoint

Actor ID	Actor	Concerns
PPArchA06	Aeroplane operator	A/C Airworthiness A/C Continuous Airworthiness
PPArchA07	Commercial Air Transport operator	Aircraft dispatch
PPArchA08	Purple Profile technical systems provider (industry)	PPArchC10
PPArchA09	Purple Profile technical systems users (stakeholders)	PPArchC10
PPArchA10	Aeronautical Certification Authorities	PPArchC10

Table 15: List of Actors interested to the deployment viewpoint

4.2.1 Functional View

The Purple Profile functional viewpoint addresses the “what” without dealing with the “where” or “how” aspects of the SWIM-TI. It mainly addresses the concern about what the Purple Profile technical systems shall/should/could do. The concern is described in terms of identification of applicable SWIM-TI functions from EATMA and functional requirements.

This section provides the architecture analysis and design. The functional requirements derived from this section are provided in §4.3.1.

4.2.1.1 Functional decomposition

The SWIM-TI functional decomposition from EATMA has been assessed and applicable functions are selected taking into account the Purple Profile SWIM Profile SPA (SWIM Profile Assertion) [Appendix A], applicable EN. The assessment of the applicability of the SWIM-TI functional decomposition from EATMA to the Purple Profile is driven by technical use cases described in §3.1.1.2, the messaging characterization [Appendix B] and the related the statement of applicability to Purple Profile provided in §B.2.1.

From the highest level of abstraction, the Purple Profile technical systems are considered as a single entity (SWIM infrastructure level) providing functions with the purpose of ensuring technical interoperability between Purple Profile enabled technical systems providing/consuming Purple Profile enabled SWIM services (§3.1.1.2). Purple Profile enabled SWIM services are characterized by the applicable technical use case and security and messaging non-functional characteristics (Table 16).

UC ID	UC Title	Aircraft role	Ground-based system role	Uplink / Downlink	(end2end) Security characteristics	(end2end) Messaging QoS characteristics
PPUC-01a	Aircraft initiated Request/Response information exchange	Consumer	Provider	Uplink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation. For a given SWIM service, each sub-characteristic is considered applicable or not and when application additional properties/parameter are specified (e.g. server-only|mutual authentication).	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection). For a given SWIM service, the required delivery guarantee is specified.
PPUC-01b	Aircraft initiated Request/Multi-Response information exchange	Consumer	Provider	Uplink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation.	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection).
PPUC-02	Ground-based system provided Publish/Subscribe information exchange	Consumer	Provider	Uplink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation.	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection).

UC ID	UC Title	Aircraft role	Ground-based system role	Uplink / Downlink	(end2end) Security characteristics	(end2end) Messaging QoS characteristics
PPUC-03a	Ground-based system initiated Request/Response information exchange	Provider	Consumer	Downlink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation.	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection).
PPUC-03b	Ground-based system initiated Request/Multi-Response information exchange	Provider	Consumer	Downlink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation.	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection).
PPUC-04	Aircraft provided Publish/Subscribe information exchange	Provider	Consumer	Downlink	Confidentiality, Authenticity (authentication) Integrity (including authorization), Accountability, Non-repudiation.	At-Most-Once (message loss) | At-Least-Once (message duplication) | Exactly-Once (message duplicates detection).

Table 16: SWIM Purple Profile technical use cases and non-functional characteristics

Following tables provide the statement of applicability to Purple Profile of the SWIM-TI functional decomposition from EATMA. As reported in Table 3~~Table 3~~ only SWIM-TI messaging and security functional blocks are applicable to this solution. EATMA SWIM-TI functions are in principle applicable to one or more SWIM Profiles. At functional view level, a function is evaluated applicable from the "what" perspective: as part of the analysis, specific constraints are identified and taken into account when specifying the corresponding technical view. Although some aspects of the "how" (e.g. standard technology) could be applicable to more than one profiles, the "how" concerning a function is profile specific.

Function	Description	Applicability to Purple Profile
Message distribution	Distribution is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEP). MEPs are mainly characterized through following attributes : - Conversation direction: a conversation is a series of related messages. The Conversation direction describes the sequencing and direction of the flow of these messages between the interacting parties . - Cardinality: it describes the number of participants in the exchange of messages. - Decoupling: it describes the degree of loose coupling between the participants. Decoupling is subdivided into 3 dimensions: - Time: Time decoupling means that the interacting parties do not have to be actively participating at the same time. - Space: Space decoupling means that the interacting parties do not have to know each other. - Synchronization: Synchronization decoupling means that the interacting parties are not blocked and can do other work. Guidance: MEPs can be composed and they exist at different levels of abstraction. Further details are provided in the P14.01.03-D39-SWIM Profiles §4.2. How different message distribution aspects behave or are configured are described via Quality of Services (reliable delivery, ordering, etc.).	Taking into account the analysis of the technical use cases, the Purple Profile SPA and the messaging characterization, this function is considered applicable. In particular, for the Purple Profile only MEPs proving time, space and synchronization decoupling are applicable. For what concerns the QoSs, the definition and the statement of applicability to the Purple Profile are provided in the messaging characterization [Appendix B] and summarized in §4.2.1.1.1. When instantiating the applicable MEPs (PSPUSH-MEP, PSPULL-MEP, FDRR-MEP and FDRMR-MEP) over the technical architecture, following constraints have to be taken into account: - Bi-directional message exchange over aircraft-initiated (TCP) connections. - Aircraft-initiated transport connectivity management (establishing, releasing, maintaining). - Store-and-forward mechanism to cope with temporary link unavailability (aircraft-ground Purple Profile interaction). - Messaging characterization statements of applicability to Purple Profile.

Message routing	The SWIM-TI Message routing is in charge of the determination of where a message will be delivered as well as defining through which communication paths a message will reach its intended destination or destinations. The decision on where a message will be delivered and through which communication paths is based on criteria. There are two main types of criteria: - Subject-based (also called header-value or meta-data) - Context-based (the context can be represented by size of the message, failure and timeout, etc.). Complex criteria can be composed by combining all types. How different message routing aspects behave or are configured are described via Quality of Services (reliable delivery, ordering, etc.).	Taking into account the analysis of the technical use cases, the Purple Profile SPA and the messaging characterization, this function is considered applicable. In particular both subject-based and context-based routing are applicable. When instantiating the message routing over the technical architecture, following constraints have to be taken into account: - Aircraft data domains segregation. - Due to aviation configuration control rules (§4.2.2.1), aircraft side message routing policies cannot be dynamically defined/updated. - Messaging characterization statements of applicability to Purple Profile (e.g. context-based routing for non-nominal cases). The technical architecture relies on the message routing function to federate aircraft and ground side messaging.
Message filtering	The SWIM-TI Message Filtering is in charge of the elimination of undesired messages based on criteria. There are two main types of criteria: - Subject-based (also called header-value or meta-data) - Context-based (the context can be represented by size of the message, failure and timeout, etc.). Complex criteria can be composed by combining all types.	Taking into account the analysis of the technical use cases, the Purple Profile SPA and the messaging characterization, this function is considered applicable. In particular both subject-based and context-based filtering are applicable. When instantiating the message filtering over the technical architecture, following constraints have to be taken into account: - Aircraft data domains segregation. - Due to aviation configuration control rules (§4.2.2.1), aircraft side message filtering policies cannot be dynamically defined/updated. - Messaging characterization statements of applicability to Purple Profile (e.g. context-based filtering for non-nominal cases). - In case of information uplink, in order to optimize the use of the aircraft and A/G network resources, the filtering should be enforced on the ground (ground side Purple Profile and/or Publisher/Responder side).

Message enrichment	The SWIM-TI Message enrichment function is in charge of adding SWIM-TI layer message properties to the message. Guidance: SWIM-TI message properties complement application layer message properties (if any). At SWIM-TI level, specific properties could be added for different purposes including but not limited to message routing, logging and QoS.	In the Purple Profile, message enrichment is currently used only for on-the-fly compression.
Messaging policy management	The SWIM-TI Messaging policy enforcement function is transversal to all the messaging functions and it allows to configure their characteristics and behaviour according to the needs (e.g. per-SWIM service QoS).	Messaging policies represent a way to properly configure functional (e.g. routing path) and non-functional (e.g. delivery guarantees) aspects specific of one messaging functions or transversal to several ones. Configurability at SWIM service level, SWIM services class of service level, etc., is considered a must to have for the Purple Profile. This allows to use the infrastructure for heterogeneous advisory information exchanges. The following messaging policies have been identified in the functional view: - Routing policy: it allows to configure routing paths. - Quality of service policy: it allows to configure messaging QoSs (§4.2.1.1.1) like durability, delivery guarantees, etc. - Compression policy: it allows to enable and configure on the fly compression at SWIM-TI layer (transparent to the Purple Profile enabled sender/publisher and consumer/subscriber applications). - Filtering policy: it allows to configure filtering criteria for both queue and topic based information exchanges. Filtering criteria provided by subscribers at subscription time are evaluated in AND relationship with any active filtering policy. Messaging policies are managed via administrative interfaces and could be updated at run-time without restarting the system/sub-system. When instantiating this function over the technical architecture, following constraints have to be taken into account: - Due to aviation configuration control rules (§4.2.2.1), aircraft side message policies cannot be dynamically defined/updated.

Company General Use

Table 17: Messaging functions applicability to Purple Profile

In Table 18 the applicability of security functions is provided. Further details are provided in §4.2.1.1.2 where the relationships between applicable and not transferred security controls and security functions are described.

Function	Description	Applicability to Purple Profile
Identity Management	The SWIM-TI Identity Management is in charge of maintaining and administrating digital identities (e.g. X.509 certificate, Security tokens): - Digital identity creation, renewal, revocation and storing. - Efficient mapping of identity to resources using a management model (e.g., role-based) and identity assignment according to an appropriate set of attributes. - Digital identity validation. - Digital identity revocation status check.	Taking into account that most of the security functions applicable to the Purple Profile rely on cryptographic mechanisms and in general on digital identity, this function is applicable to the Purple Profile (see note 1 for air side specificities). This function is provided by dedicated CC/Technical systems external to the Purple Profile: security functions are expected to able to properly interact with IdM's capabilities (e.g. digital identity revocation status check).
Authentication	The SWIM-TI Authentication function is in charge of the verification of the claimed identity evaluating additional information (authentication credentials) that is bound to this identity and can only be provided by an entity with that identity.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile (see note 1 for air side specificities). This function is used for mutual authentication between messaging entities: - Sender and Message Queue, - Receiver and Message Queue, - Publisher and Message Topic, - Subscriber and Message Topic, - Subscriber and subscription handler.
Authorization	The SWIM-TI Authorization function is in charge of granting of rights and, based on these rights, granting of access to resource.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile (see note 1 for air side specificities). This function is used to grant access to message queue, message topic and subscription handler only to authorized senders/receivers/publishers/subscribers.

Audit	The SWIM-TI Audit function is in charge of audit records/events generation concerning security related actions and events. In particular it allows to create, submit, persistently store and report on audit events. This function aims at enabling the proof of action, proof of data source, etc.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile (see note 1 for air side specificities).
Confidentiality ensuring	The SWIM-TI Confidentiality ensuring function is in charge of enabling the protection of information in transmission from unauthorized access relying on cryptographic mechanisms.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile (see note 1 for air side specificities).
Information Integrity and authenticity ensuring	The SWIM-TI Information integrity and authenticity ensuring function is in charge of enabling the verification of both integrity and authenticity of the information in transmission relying on cryptographic mechanisms.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile (see note 1 for air side specificities).
Message screening	The SWIM-TI Message screening function is in charge of screening messages in order to filter out messages with malicious or malformed content.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile. Message screening is also dealing with typed queue and typed topic concepts: a typed message queue (or topic) is a queue for which only predefined message type(s) are allowed. Message screening allows to protect the recipients of the message against unexpected message types.
Overload protection	The SWIM-TI Overload protection function is in charge of limiting resources utilization according to specific criteria to avoid failures due to insufficient resources. Criteria are specified via threshold and they could be of following types: - Maximum message size, - Maximum message rate, - Maximum concurrent connection number, - Maximum number of pending messages to be processed.	Taking into account the Security risk assessment, this function is considered applicable to the Purple Profile.

Security Policy management	The SWIM-TI Security policy enforcement function is transversal to all the security functions and it allows to configure their characteristics and behaviour according to the needs (e.g. per-message queue authorization).	Security policies represent a way to properly configure aspects specific security functions or transversal to several ones. Configurability at SWIM service level, SWIM services class of service level, etc., is considered a must to have for the Purple Profile (see note 1 for air side specificities). This allows to use the infrastructure for advisory information exchanges with different constraints in terms of security controls enforcement. The following security policies have been identified in the functional view: - Authentication policy: it allows to configure digital identity information including identity type and attributes. - Authorization policy: it allows to configure role based authorization rights. - Confidentiality, integrity and authenticity policies: they allow to configure aspects like cryptographic protocols, algorithms and cipher suites. - Message screening policy: it allows to enabled/disable and property configure aspects like screening rules (warning, drop, etc.) and reference schema and assertions for validating messages. - Overload protection policy: it allows to property configure aspects like maximum concurrent consumers, maximum message size, alerting rules (warning, etc.). - Audit policy: it allows to properly configure aspects like when and what information have to be logged, etc. Security policies are managed via administrative interfaces and some of them (authorization) could be updated at run-time without restarting the system/sub-system. However, due to aviation configuration control rules (§4.2.2.1), aircraft side security policies cannot be dynamically defined/updated.

Table 18: Security functions applicability to Purple Profile

Note1: When instantiating these functions over the technical architecture, aircraft specific constraints and rules of the air regulations have to be taken into account. The technical view provides more details on this external interface.

4.2.1.1.1 Messaging Quality of service

Service level NFRs are provided in the Service Definition (NFR and QoS terms are often used as synonyms). Services require different classes of performance and functionalities, thus different message distribution classes of service (CoS) levels may be defined.

Currently there is no SESAR2020 level QoS/NFR framework/ontology defining how and what to specify at service level and how these service level needs are mapped to SWIM-TI functional and non-functional requirements (e.g. NFR at service level may result in FRs and NFRs at SWIM-TI level). On the other hand, the SWIM Profiles definition [52] is based on NFR characterization derived from ISO/IEC 25010. In particular it includes a NFR ontology and NFR identification "checklist" applicable to the SWIM-TI level. As part of the messaging characterization [Appendix B] several characteristics/QoSs concerning entities participating to information exchange have been defined. This was required because currently there are no major global well-known standardisation entities that have created an exhaustive ontology/terminology for messaging QoS (technology standards and products use their own localised ontologies/models). Starting from this ontology, the QoSs applicable to the Purple Profile have been identified (statement of applicability in Appendix B). These QoSs are further detailed in the remaining part of this section. It is anticipated that for some QoS, the PP provides different options: the option better fitting the needs is selected according to the service level NFRs taking into account recommendations about the combination of different QoS (not all the possible combination make sense/are recommended). Furthermore, the QoSs have to be properly configured across all the entities involved in Purple Profile enabled SWIM services provision and consumption.

4.2.1.1.1.1 Lifespan/Lifetime

In Table 19 the Lifespan/Lifetime QoSs provided by the PP are described. Relationships between this QoS, entities and events are described in table 10 in the messaging characterization [Appendix B]. These relationships are part of the functional view and are taken into account in the design of the technical view. The statement of applicability to Purple Profile of these characteristics is provided in §B.2.1 (it includes also mandatoriness and mandatoriness levels).

Entity	Lifespan/Lifetime QoS	Note
Message	Message with non-zero/specified lifespan	In order to avoid message starvation in MQ and MT (resources saving) messages which will not expire are not allowed in the PP. This design decision is also coherent with the fact that advisory information (AI/MET) have typically a limited lifetime. Expired messages are filtered out and routed according to the applicable context-based routing policy. Messages with undefined expiration time should be rejected or a default expiration time should be added. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
Message Queue	Non-Temporary Queue	Only Non-Temporary Queues are allowed. Mandatoriness: mandatory.

Company General Use

		Mandatoriness level: N/A (it is not optional)
Message Topic	Non-Temporary Topic	Only Non-Temporary Topics are allowed. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional).
Subscription	Subscription with zero/unspecified lifespan	It is always required to perform the unsubscription. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Subscription with non-zero/specified lifespan	As advanced QoS it is possible to provide subscription with specified/default expiration time. This advanced feature could be useful for some specific services (protecting consumption of resources allocated to subscribers which do not unsubscribe) and/or subscribers. A cons is that the expiration time provided by the subscriber could not be always fitting its needs (duration of the subscription) leading to the need to renew the subscription / subscribe again. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced capabilities that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).

Table 19: Purple Profile Lifespan/Lifetime QoS

4.2.1.1.1.2 Ordering guarantees

In Table 20 the Ordering guarantees QoSs provided by the PP are described. Relationships between this QoS, entities and events are described in table 12 in the messaging characterization [Appendix B]. These relationships are part of this functional view and are taken into account in the design of the technical view. The statement of applicability to Purple Profile of these characteristics is provided in §B.2.1 (it includes also mandatoriness and mandatoriness levels).

Entity	Ordering guarantees QoS	Note
Message	Message priority	At service level it is possible to indicate that messages have different priorities (end to end). To guarantee that this property is covered end to end, it is needed to select the Message Priority based ordering for Message Queue or Message Topic. It makes no sense to use message priority and to select FIFO ordering for Message Queue or Message Topic. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).

	Message with default priority	At service level it is possible to indicate that messages have no priority (default priority). In this case it makes no sense to select the Message Priority based ordering for Message Queue or Message Topic. The FIFO ordering should be used.
Message Queue	FIFO	At service level it is possible to indicate that Message Queue FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. Furthermore, this QoS has to be the same for all the MQs part of the bindings triad concerning the specific service. This to guarantee the end to end FIFO ordering. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Message Priority (best effort)	At service level it is possible to indicate that Message Priority based Message Queue ordering is needed. This QoS makes sense only if Message level priority QoS is required. Furthermore, this QoS has to be the same for all the MQs part of the bindings triad concerning the specific service. This to guarantee the end to end FIFO ordering. The strict priority ordering is not required: best effort ordering is required meaning that realizations of this QoS should be stricter as possible. Several options could be identified at technical level. One could be to assign priority to Message queues each with FIFO ordering strategy in a way transparent to the sender and the receiver. In order to prevent starvation of messages in the low priority queue, the intermediary applies as sort of round-robin scheduling (this schema cannot ensure the strict ordering). Depending on the assessment of the interoperability needs, in the technical view specific design solutions could specified or not. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).
Message Topic	FIFO	At service level it is possible to indicate that Message Topic FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. Furthermore, this QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end FIFO ordering. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Message Priority (best effort)	At service level it is possible to indicate that Message Priority based Message Topic ordering is needed.

Company General Use

		This QoS makes sense only if Message level priority QoS is required. Furthermore, this QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end FIFO ordering. Similar considerations provided for Message Queue priority-based ordering QoS are also applicable to Message Topic priority-based ordering QoS. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).

Table 20: Purple Profile Ordering guarantees QoS

4.2.1.1.1.3 Durability

In Table 21 the durability QoSs provided by the PP are described. Relationships between this QoS, entities and events are described in table 11 in the messaging characterization [Appendix B]. These relationships are part of this functional view and are taken into account in the design of the technical view. The statement of applicability to Purple Profile of these characteristics is provided in §B.2.1 (it includes also mandatoriness and mandatoriness levels).

Entity	Durability QoS	Note
Message	Durable (recommended)	At service level it is possible to indicate that durable messages are needed (end to end). This QoS has to be properly combined with durability configured for the other entities in order to guarantee the end to end needs. For instance there are no guarantees for durable messages sent to non-durable MQ. This is the recommended message durability QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Non-Durable	At service level it is possible to indicate that durable messages are not needed (end to end). In this case it makes no sense to select the Durable Message Queue or Message Topic QoS. Volatile or non-durable MQ/MT should be used. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
Message Queue	Non-Durable	At service level it is possible to indicate that Message Queue Non-Durable durability is needed. This QoS makes sense only if at non-durable messages QoS is required at message level.

		Furthermore, this QoS has to be the same for all the MQs part of the bindings triad concerning the specific service. This to guarantee the end to end QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Volatile	At service level it is possible to indicate that Message Queue Volatile durability is needed. This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). Furthermore, this QoS has to be the same for all the MQs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. The case where one or more of the MQs part of the triad have different durability (e.g. Non-durable, durable) is not considered in this specification. The expected end to end behaviour is not described. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Durable (recommended)	At service level it is possible to indicate that Message Queue Durable durability is needed. This QoS has to be the same for all the MQs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. This is the recommended MQ durability QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
Message Topic	Non-Durable	At service level it is possible to indicate that Message Topic Non-Durable durability is needed. This QoS makes sense only if at non-durable messages QoS is required at message level. Furthermore, this QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Volatile	At service level it is possible to indicate that Message Topic Volatile durability is needed. This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). Furthermore, this QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. The case where one or more of the MTs part of the triad have different durability (e.g. Non-durable, durable) is not considered in this specification. The expected end to end behaviour is not

Company General Use

		described. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Durable (recommended)	At service level it is possible to indicate that Message Topic Durable durability is needed. This QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. This is the recommended MT durability QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
Subscription	Non-Durable (Not applicable to aircraft subscriptions)	At service level it is possible to indicate that non-durable subscription QoS is needed. In general, service level requirements may or may not constrain this QoS. It could be possible to allow both durable and non-durable subscriptions demanding to the specific subscribers to select the right durability. However, taking into account that aircraft PP SWIM Node are not always connected to the ground PP SWIM Node, this QoS is not allowed for aircraft subscriptions. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Durable (recommended)	At service level it is possible to indicate that durable subscription QoS is needed. In general, service level requirements may or may not constrain this QoS. It could be possible to allow both durable and non-durable subscriptions demanding to the specific subscribers to select the right durability. However, taking into account that aircraft PP SWIM Node are not always connected to the ground PP SWIM Node, this QoS is mandatory for aircraft subscriptions. Ground applications subscribing to aircraft provided services may decide to use durable or non-durable subscriptions (assuming the service design will not constrain this QoS). However, this is the recommended Subscription durability QoS also for ground subscriptions. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
Subscription handler	Volatile	At service level it is possible to indicate that Subscription handler Volatile durability is needed. This QoS does not guarantees that subscriptions are not lost irrespective of the subscription level durability QoS (durable or non-durable). Furthermore, this QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. The case where one or

		more of the MTs part of the triad have different durability (e.g. Non-durable, durable) is not considered in this specification. The expected end to end behaviour is not described. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	Durable (recommended)	At service level it is possible to indicate that Subscription handler Durable durability is needed. This QoS has to be the same for all the MTs part of the bindings triad concerning the specific service. This to guarantee the end to end durability level. This is the recommended Subscription handler durability QoS. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced durability level that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).

Table 21: Purple Profile durability QoS

4.2.1.1.1.4 Delivery guarantees

In Table 22 the delivery guarantees QoSs provided by the PP are described. In the messaging characterization [Appendix B] §3.4.3.2 following relationships are described:

- (Table 13) Point-to-point delivery guarantees, lifetime and durability QoSs.
- (Table 14) End-to-end guarantees, point-to-point delivery guarantees, lifetime and durability QoSs.
- (Table 15) Non-nominal events, end-to-end and point-to-point delivery guarantees QoSs.

These relationships are part of this functional view and are taken into account in the design of the technical view. For further details refer to the messaging characterization [Appendix B]. Furthermore it is anticipated that At-Least-Once and Exactly-Once delivery guarantees cover recoverable or transient faults only. To enable Exactly-Once delivery guarantees is a necessary but not always sufficient condition for message delivery: some faults such as network partitioning/isolation may not allow to deliver the message because permanent failure and/or because the message expires while recovering (refer to messaging characterization [Appendix B]). The statement of applicability to Purple Profile of these characteristics is provided in §B.2.1 (it includes also mandatoriness and mandatoriness levels).

Delivery guarantees	Delivery guarantee	Note
Point-to-point	At-Most-Once	Depending on the service level NFRs, it is possible to indicate that the At-Most-Once point to point delivery guarantees QoS is

		needed. End to end PP information exchange chain is composed by a binding triad and, in the most general case, by three connections. For a given service, each of these connections may be configured using different connection level delivery guarantees QoS. This freedom is constrained by the required end to end delivery guarantees QoS. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	At-Least-Once (recommended)	Depending on the service level NFRs, it is possible to indicate that the At-Least-Once point to point delivery guarantees QoS is needed. This is the recommended point to point delivery guarantee QoS. End to end PP information exchange chain is composed by a binding triad and, in the most general case, by three connections. For a given service, each of these connections may be configured using different connection level delivery guarantees QoS. This freedom is constrained by the required end to end delivery guarantees QoS. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced durability level that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).
	Exactly-Once	Depending on the service level NFRs, it is possible to indicate that the Exactly-Once point to point delivery guarantees QoS is needed. End to end PP information exchange chain is composed by a binding triad and, in the most general case, by three connections. For a given service, each of these connections may be configured using different connection level delivery guarantees QoS. This freedom is constrained by the required end to end delivery guarantees QoS. Exactly-Once delivery guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced durability level that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).
	No delivery guarantees (Not allowed for air-ground connections)	Depending on the service level NFRs, it is possible to indicate that no point to point delivery guarantees are needed. End to end PP information exchange chain is composed by a binding triad and, in the most general case, by four connections. For a given

Company General Use

		service, each of these connections may be configured using different connection level delivery guarantees QoS. This freedom is constrained by the required end to end delivery guarantees QoS. However, this connection level delivery guarantees QoS is not applicable to air-ground connections. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
End-to-end	At-Most-Once	Depending on the service level NFRs, it is possible to indicate that the At-Most-Once end to end delivery guarantees QoS is needed. This is an end to end QoS constraining the connection level and durability QoS. Because this end to end QoS does not guarantee that messages are not lost, the bindings triad can be configured using non-durable, volatile or durable MQ/MT/Subscription handler durability QoS. In order to save resources, it is recommended to do not use durable MQ/MT/Subscription handler when At-Most-Once end to end delivery guarantees QoS is used. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)
	At-Least-Once (recommended)	Depending on the service level NFRs, it is possible to indicate that the At-Least-Once delivery guarantees QoS is needed. This is the recommended end to end delivery guarantees QoS. This is an end to end QoS constraining the connection level and durability QoS. Because this end to end QoS guarantee that messages are not lost, the bindings triad shall be configured using durable MQ/MT/Subscription handler durability QoS. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced durability level that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.*).
	Exactly-Once	Depending on the service level NFRs, it is possible to indicate that the Exactly-Once delivery guarantees QoS is needed. This is an end to end QoS constraining the connection level and durability QoS. Exactly-Once delivery guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability. Mandatoriness: optional. Mandatoriness level: Optional Profile part (*Advanced durability level that could be*

		allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.).
	No delivery guarantees	Depending on the service level NFRs, it is possible to indicate that no end to end delivery guarantees are needed. In this case there are no constraints on the connection level and durability QoS used. Mandatoriness: mandatory. Mandatoriness level: N/A (it is not optional)

Table 22: Purple Profile Delivery guarantees QoS

4.2.1.1.2 Security Risk assessment and security functions

This section provides the relationships between applicable and not transferred security controls and security functions. Additional security controls have been considered applicable (meaning that they have to be properly addressed in development and deployment phases) but they have been transferred to a third-party according to the limited scope of this solution (technological/technological solution).

As reported in Table 23 not all the security controls (e.g. CAT_CTRL_100) are “covered/traced” by SWIM-TI security functions (for which requirements are provided in both functional and technical views). The main reasons are (i) the (limited) purpose of the SWIM-TI security functional view (Figure 27) and (ii) that such security controls concern more the technical viewpoint. For these security controls, design and requirements are provided in the Purple Profile technical view.

It has to be noted that Purple Profile security functional and technical views represent a sub-set of the overall security management. In particular, in addition to requirements provided in this specification, the complete picture should address following aspects:

- All the applicable but transferred security controls.
- All the additional supporting assets not addressed by this specification.
- All the security related deployment and operational aspects not addressed by this specification.

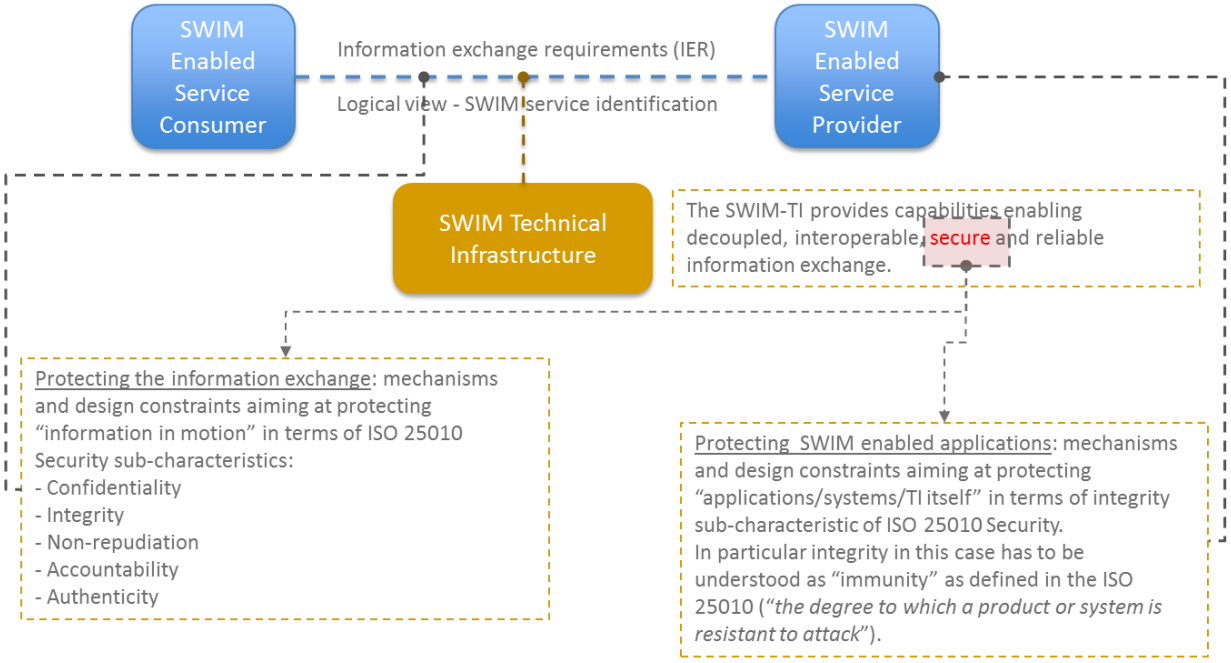


Figure 27: SWIM-TI Security functional view

Security Control ID (s)	Security Control Name(s)	Applicability rationale	Function(s)
CAT_CTRL_167	Information transfer policies and procedures (ISO 27002:2013)	PJ.17-01, as technological solution, will define controls and controls configuration. Policies and procedures for operational consumption and provisioning of SWIM services are not covered by this solution.	Identity Management, Authentication, Authorization, Audit, Confidentiality ensuring, Information Integrity and authenticity ensuring, Security Policy enforcement.
CAT_CTRL_020 CAT_CTRL_169	Information transfer 2 Electronic messaging (ISO 27002:2013)	PJ.17-01 will define controls and controls configuration to enable the proper protection of electronic messaging.	Identity Management, Authentication, Authorization, Audit, Confidentiality ensuring, Information Integrity and authenticity ensuring, Security Policy enforcement.
CAT_CTRL_022 CAT_CTRL_150	Logging and Monitoring 2 Event logging (ISO 27002:2013)	PJ.17-01 will define (technical view) controls to protect logging facilities and log information against tampering and unauthorized access.	None. Most of the security functions aim at enabling protection of information transfer.

CAT_CTRL_023 CAT_CTRL_151 CAT_CTRL_152	Logging and Monitoring 3 Protection of log information Administrator and operator logs	PJ.17-01 will define (technical view) requirements for logging dealing with a limited set of "corrective actions" (non-nominal cases identified by the solution). Complete procedure for analysing and reporting all the possible faults is required but not covered by this solution.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_153	Clock synchronisation	PJ.17-01 will define (technical view) requirements for time representation, synchronisation and accuracy.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_026	Media handling 3	PJ.17-01 will define (technical view) controls to protect access control to storage resources. Procedure handling and storage of ATM information is required but not covered by this solution.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_100	Access control policy (ISO 27002:2013)	PJ.17-01 provides requirements (technical view) to protect the access to ATM services, information and information processing facilities. The solution is not dealing with procedures for establishing and managing policies.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_112	Information access restriction (ISO 27002:2013)	PJ.17-01 provides requirements (technical view) to restrict access to SWIM functions administration.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_113	Secure log-on procedures (ISO 27002:2013)	PJ.17-01 provides requirements (technical view) to restrict access to SWIM functions administration.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_115	Use of privileged utility programs (ISO 27002:2013)	PJ.17-01 provides requirements (technical view) to restrict and tightly control the use of utility programs that might be capable of overriding configurations and security controls.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_119	Policy on the use of cryptographic controls (ISO 27002:2013)	All the security functions concern cryptographic controls. PJ.17-01 provides requirements concerning the use of such controls (recommended algorithms, etc.). The solution is not dealing with procedures for establishing and managing policies.	Identity Management, Authentication, Authorization, Audit, Confidentiality ensuring, Information Integrity and authenticity ensuring, Security Policy enforcement.

CAT_CTRL_120	Key management (ISO 27002:2013)	All the security functions concern cryptographic controls based on security keys. PJ.17-01 provides requirements concerning the use of such controls. The solution is not dealing with procedures for establishing and managing policies. Furthermore, this solution is also not dealing with detailed technical requirements concerning CA/Identity provider (e.g. CRL maintenance, X.509v3 specific profiles, etc.). These aspects are part of the overall security management to be further detailed taking into account actual deployment.	Identity Management, Authentication, Authorization, Audit, Confidentiality ensuring, Information Integrity and authenticity ensuring, Security Policy enforcement.
CAT_CTRL_208	Implementing information security continuity (ISO 27002:2013)	PJ.17-01 provides reliability, message screening and overload protection requirements representing a basis for information security continuity. The solution is not dealing with procedures for establishing and managing policies.	Message screening, Overload protection. Durability and delivery guarantees messaging QoS (Message distribution function).
CAT_CTRL_211	Availability of information processing facilities (ISO 27002:2013)	PJ.17-01 provides reliability, message screening and overload protection requirements representing a basis for protecting information processing availability. The solution is not dealing with procedures for establishing and managing policies.	Message screening, Overload protection. Durability and delivery guarantees messaging QoS (Message distribution function).
CAT_CTRL_157	Management of technical vulnerabilities (ISO 27002:2013)	PJ.17-01 provides requirements about periodic independent vulnerability assessment. Additional aspects concerning security organization and procedures are not covered by this solution.	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_028	Network security management 1	From network user perspective, PJ:17-01 could provide requirements (allocated to the network) to "maintain security for the ATM systems and applications using the network, including information in transit".	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_163	Network controls (ISO 27002:2013)	From network user perspective, PJ:17-01 could provide requirements (allocated to the network) to "maintain security for the ATM systems and applications using the network, including information in transit".	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_164	Security of network services (ISO 27002:2013)	From network user perspective, PJ:17-01 could provide requirements (allocated to the network) to "maintain security for the ATM systems and applications using the network, including information in transit".	None. Most of the security functions aim at enabling protection of information transfer.

CAT_CTRL_101	Access to networks and network services (ISO 27002:2013)	From network user perspective, PJ:17-01 could provide requirements (allocated to the network) to "maintain security for the ATM systems and applications using the network, including information in transit".	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_165	Segregation in networks (ISO 27002:2013)	From network user perspective, PJ:17-01 could provide requirements (allocated to the network) to "maintain security for the ATM systems and applications using the network, including information in transit".	None. Most of the security functions aim at enabling protection of information transfer.
CAT_CTRL_053	Security requirements of information systems 1	PJ.17-01 provides security requirements in accordance with the security risk assessment .	All the functions plus security technical view.
CAT_CTRL_173	Information security requirements analysis and specification (ISO 27002:2013)	PJ.17-01 provides security requirements in accordance with the security risk assessment .	All the functions plus security technical view.

Table 23: Security functions and SESAR2020 SCs

End-to-end security is an important aspect in particular in this context where the SWIM-TI (Purple Profile) plays the role of intermediary between the aircraft applications and the ground-based applications consuming/providing services. In order to guarantee end-to-end security, transport level security cryptographic techniques have to be properly combined with message level security techniques. Transport level security (with respect to message level) only guarantees point to point confidentiality, integrity and authenticity (e.g. between endpoints used by aircraft and ground Purple Profile capabilities to interact with each other).

And finally, some SWIM services operated on the SWIM-TI (Purple Profile) could also introduce security controls at application level (for a service requiring a specific point to point or distributed security control).

4.2.1.1.3 Layered functional view

In Figure 28 the Purple Profile layered functional view is depicted:

- Technical system(s) belonging to the Aircraft CC rely on Purple Profile functions to consume or provide Purple Profile enabled SWIM services. The Technical system is Purple Profile enabled in the sense that it is capable of interact with the infrastructure (Purple Profile enabled application messaging and security capabilities).
- Technical system(s) belonging to generic ground CC (e.g. Regional AIM, ATM-MET, etc.) rely on Purple Profile functions to consume or provide Purple Profile enabled SWIM services. The Technical system is Purple Profile enabled in the sense that it is capable of interact with the infrastructure (Purple Profile enabled application messaging and security capabilities).
- The Purple Profile technical systems provide messaging and security capabilities introduced above (Table 17 and Table 18) and it relies on:

- Identity Management CC for digital identity management (e.g. revocation status check).
- Communication network infrastructure for network level capabilities (IP routing, etc.).

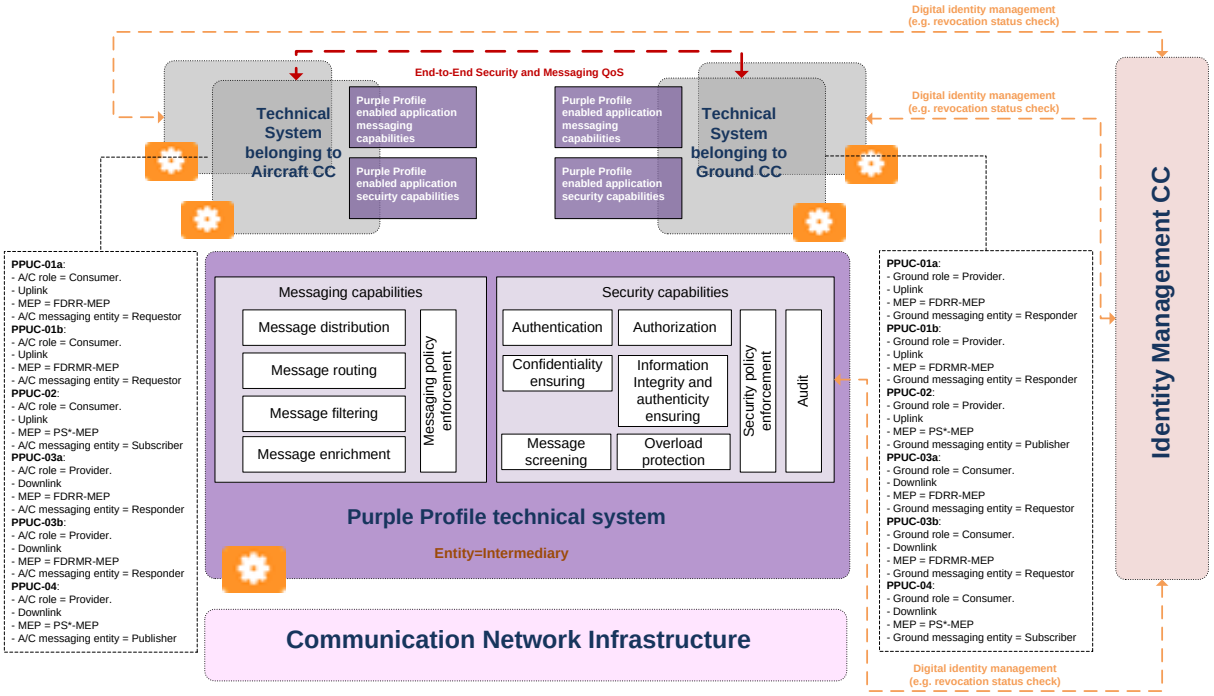


Figure 28: Purple Profile layered functional view

For each of technical systems in Figure 28, additional information is provided per technical use case: the role, messaging entity, MEP and information direction are reported. This allows to link, at functional view level, the functional layered architecture, technical use cases and messaging characterization.

It is anticipated that the communication network infrastructure in Figure 28 (functional view), is a complex infrastructure further decomposed in the technical view in three different IP-based communication network infrastructures:

- Aircraft information network used to interconnect aircraft AISD applications, SWIM-TI capabilities and A/G Communication Network.
- A/G Communication Network Infrastructure used to interconnect the aircraft SWIM-TI capabilities with the ground SWIM-TI.
- G/G Communication Network Infrastructure(s) used to interconnect the ground SWIM-TI and ground ATM Applications.

As anticipated above (Table 17 and Table 18), the technical view has to take into account constraints due to the involvement of the Aeroplanes. In particular, aeroplanes design must comply with European Aviation Safety basic regulation (EC N°216/2008 implementing rules) for:

- Initial Airworthiness (EC N°1702/2003)
- Continuous Airworthiness (EC N°2042/2003)

As such, aircraft side SWIM design must consider European Aviation Safety Agency (EASA) Certification specifications (CS) for initial airworthiness, Notices for proposed Amendments (NPA), Acceptable Means of Compliance (AMC), airworthiness Directive (AD), continuous airworthiness review items (CARI), Safety Information Bulletin (SIB), etc.

In addition, Air transport operation must consider European common technical requirements and administrative procedure applicable to commercial transportation by Aeroplane (EU OPS1, EC N°859/2008).

Thus, aircraft side SWIM, holds specificities, as it has to comply with Aircraft architectural principles (e.g. safety, configuration control and maintainability, cybersecurity) applicable to data link systems, for which:

- Avionics Safety: safety objectives are needed at TRL6 level to ensure that compliance to EASA main airworthiness requirement is reachable when considering the integration of SESAR PP AIR AG SWIM AP to aircraft systems, even if the solution targets “non-safety aeronautical information services”. This is addressed in §4.2.2.1 and §4.3.6.
- Avionics Configuration control and Maintainability: Aircraft maintenance and configuration control is done under the Continuing Airworthiness Management Organisation (CAMO) regulation (Part M, Part 145). Aircraft maintenance is either regular scheduled (heavy, light …) or unscheduled (under MMEL directives) accordingly to the Aircraft technical documentation. This is addressed in §4.2.2.1 and §4.3.2.
- Avionics Security: Network security is the responsibility of avionics system integrator to meet airline/network service provider and must comply with airline security policy for remote operations and third-party information exchange. This is addressed in §4.2.2.1 and §4.3.5.

  As cyber security technologies may be subject to export controls, it is the responsibility of operators that might export technology to be aware of the steps necessary to ensure that their operations are lawful.

  US export control considered in aviation involves two kinds of regulation, International Traffic in Arms Regulations (ITAR), and Export Administration Regulations (EAR). The latter may be applicable to cyber components, depending how they are operated. In Europe, EEC export control regime is governed by Regulation (EC) No 428/2009.

  These regulations mainly call for a self-assessment against control lists, which is categorized. As an example, for US EAR, information technologies fall in category 5, whereas avionics falls in category 7. Thus, public equipment and avionics may have different classifications for the same technology, depending on countries’ regulations.

  As a result, Aircraft operators should consider SWIM cyber security technologies usage to conduct their export control self-assessment.

Abovementioned constraints, and additional ones, are taken into account when detailing the functional view:

- Some of these constraints are covered in design and specification decisions (technical view).
- Some of these constraints are covered by design and construction constraints requirements ((technical view)
- Some of these constraints are further detailed as part of the deployment view (e.g. applicable installation options for on board SWIM).

4.2.1.2 Interface Identification

At functional view level no technical interfaces could be identified/described. At this level of abstraction the external interfacing layers are identified and then properly detailed in the technical view (interface bindings, §C.1.1 and §4.2.2). Starting from the layered view depicted in Figure 28, the three interfacing layers depicted in Figure 29 have been identified.

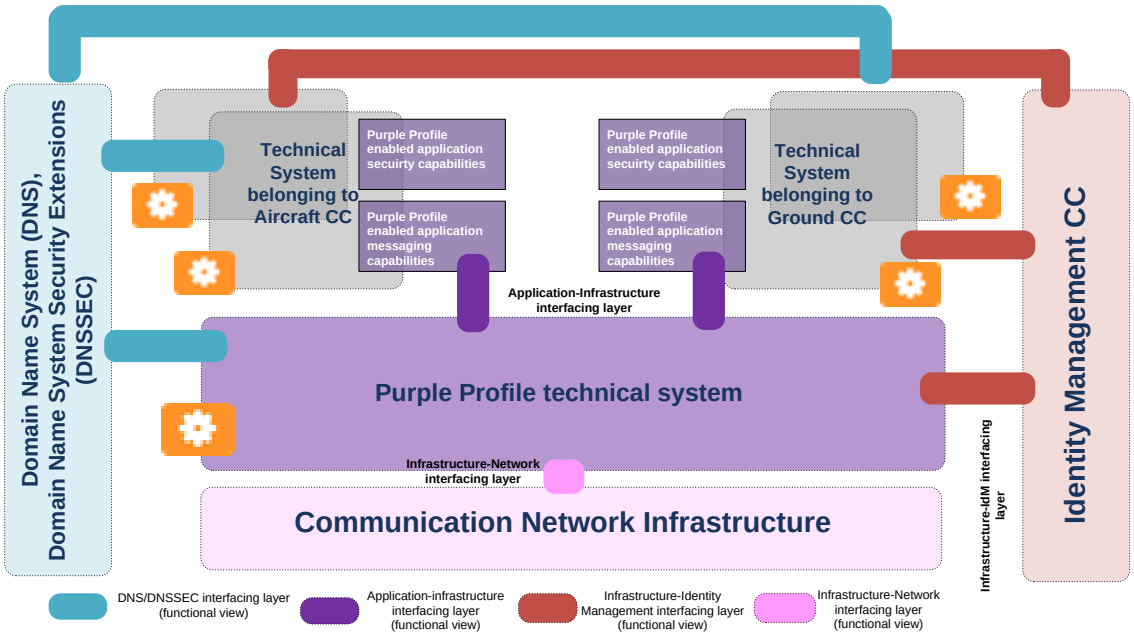


Figure 29: Purple Profile layered functional view interfacing layers

Application-infrastructure interfacing layer aims at allowing the Purple Profile enabled application to send/receive messages according to applicable technical use case (Table 16).

Infrastructure-Identity Management (IdM) interfacing layer aims at allowing the infrastructure's security functions to check digital identity validation, revocation status, etc. Similar interfacing layer can be identified also between Purple Profile enabled applications and IdM.

The SWIM-TI not only provides the messaging functionality between SWIM enabled technical systems but, in order to be able to do so, it also needs to enable interaction between consumers and

providers of supporting services. Because of differing degrees of freedom, lifecycle and governance, this interaction is sub-structured in two distinct forms: interaction with supporting services inside the SWIM-TI and interaction with supporting services outside the SWIM-TI. An example of the former could be a DNSSEC service specific for and proprietary to the SWIM-TI. An example of the latter could be a PKI infrastructure that is not only used by the SWIM-TI but also by the IP Network (for instance IPsec) and/or the SWIM Enabled technical systems (for instance data signing).

It has to be noted that Purple Profile security functional and technical views represent a sub-set of the overall security management. In particular, in addition to requirements provided in this specification, additional aspects should addressed (§4.2.1.1.2).

Infrastructure-network interfacing layer aims at allowing the infrastructure to interact with the underlying IP Network (e.g. establish TCP/IP connection, interacting with IdM, DNSSEC, etc.). It is a given that the SWIM-TI does not deal with the IP Network layer: by definition the scope of the SWIM-TI stops at the IP Network layer. The SWIM-TI interacts with the IP Network layer in a manner conforming to the contract and the IP Network layer provides an abstraction for the SWIM-TI from the complexity of underlying networking technology. Currently two types of IP Network layers are considered: an IPv4 layer and an IPv6 layer. Besides common functionality such as routing, the IP Network layers may also provide security controls such as IP-address filtering and IPsec tunnelling. The presence of such security controls is transparent for the SWIM-TI.

Although not depicted in Figure 29, the Purple Profile infrastructure requires administration capabilities to properly configure messaging and security functions.

4.2.2 Technical View

The Purple Profile technical viewpoint complements and specializes the “what” aspect (functional viewpoint, §4.2.1) addressing the “how” and “how good” but without dealing with the “where” aspects of the SWIM-TI. It provides the technical view according to technical architecture and technical interoperability needs (“how”) and SWIM-TI’s NFRs (“how good”). It mainly addresses the concern about how to realize the sub-set of functions according to interoperability needs assessment. The concern is described in terms technical architecture definition, SWIM interface binding, technical and non-functional requirements.

This section provides the technical architecture analysis and design. Requirements concerning this view are provided in §4.3.2-§4.3.7.

At functional viewpoint, the Purple Profile technical systems are considered as a single entity (SWIM infrastructure layer) providing functions with the purpose of ensuring technical interoperability between Purple Profile enabled technical systems providing/consuming Purple Profile enabled SWIM services. These functions concerns the Application-infrastructure interfacing layer described in §4.2.1.2. At technical view level, the component that provides/realizes/deploys the functions of the functional view is the SWIM Node: an autonomous point of presence in the Distributed System (of Systems) that interacts with other SWIM Nodes in the Distributed System (of Systems). This point of presence makes a set of functionality via one or more SWIM Nodes available to any SWIM Node or allows use of the functionality that is made available by a SWIM Node via one or more SWIM Nodes. The autonomy of a SWIM Node reflects the freedom (implementation choices such as but not limited to hardware/virtualisation, OS, high availability techniques and platform) and governance (such as but not limited to development process, running of operations and definition of policies).

Form architectural point of view, each of the technical systems introduced in §3.1.1 is modelled as SWIM Node:

- Ground Purple Profile Technical System: Ground Purple Profile SWIM Node.
- Air Ground Purple Profile Technical System: Air Purple Profile SWIM Node.

A SWIM Node makes the applicable functions available via one or more protocol stacks defined in the SWIM-TI scope: at the top of the protocol stack one find the consumers and providers and at the bottom one finds the IP Network layers. Such protocol stack is the basis of the SWIM-TI notion interface “binding” (conceptual relationships between Purple Profile and SWIM Services is introduced in §3.1.1.2). A SWIM-TI “binding” is:

- a particular grouping and linking of distinct protocols
- a particular mandated behaviour
- description of the interfacing

Taking into account that a given protocol stack could be used to provide/consume different SWIM services, the binding is enriched with a “contract” field that lists design artefacts (when applicable) to be documented when instantiating a give SWIM service over that binding. For instance, a binding for sharing XML data over a protocol stack with rich set of QoSs could require as part of the “contract” filed that XSDs and applicable QoSs have to be documented when instantiating a give SWIM service over that binding.

As described in §4.2.1.2, the SWIM-TI not only provides the messaging functionality between SWIM enabled technical systems but to be able to do so it also needs to enable interaction between

Company General Use

consumers and providers of supporting services. Also in these cases, standard based bindings are defined.

Taking into account the above, currently, following interface binding types are defined in the context of SWIM-TI:

- <Service binding>. Binding external to the SWIM-TI and used to consume/provide SWIM service only.
- <Internal service binding>. Binding internal to the SWIM-TI and related to internal services/messaging (e.g. messaging federation at SWIM-TI layer).
- <External service binding>. Binding external to the SWIM-TI (e.g. Time Service, CA services) and not a <Service binding> or a <Network binding>.
- <Network binding>. Binding external to the SWIM-TI and related to the IP Network layers only.

For each such SWIM-TI "binding" a single umbrella requirement is defined. The purpose of a single SWIM-TI "binding" requirement is to provide sufficient detail to promote independent unsynchronised development and/or configuration of the SWIM-TI "binding" by multiple distinct Stakeholders, resulting in an out of the box Plug & Play interoperability.

Bindings applicable to the Purple Profile are identified, described and specified in the technical view. In particular their identification and description are provided in the sections below whereas binding requirements are provided in §4.3.7.

General bindings guidance is provided in C.1.1.

4.2.2.1 Avionics architectural considerations

This section addresses avionics specificities described in §4.2.1, and provides the technical aspects governing avionics architectural choices.

4.2.2.1.1 Aeroplanes categorization

Considering Air operations regulation in EEC, EASA air operations (Air OPS) regulatory package (965/2012 and associated amendments) considers commercial air transport (CAT) operations with aeroplanes and helicopters, non-commercial operations (NCC) with aeroplanes, helicopters, balloons and sailplanes, and general aviation operation (NCO).

Note that unmanned aircraft operations are not actually considered in this categorization.

Initial Airworthiness categorization of aeroplanes, considered by this solution, supporting theses operations is resulting from EASA Certification parts:

- Large Aeroplanes (Mainline aircraft): Turbine powered Large Aeroplanes supporting CAT operation, certified under EASA CS-25 part.
- Light Aeroplanes (Regional aircraft): Light aeroplanes supporting CAT operation, either certified under EASA CS-25 (more than 19 seats and T/O weight greater than 19000 pounds) or CS-23 part (less than 19 seats and T/O weight less than 19000 pounds).
- Light Aeroplanes (Business aircraft): Light aeroplanes supporting CAT or NCC operation, certified under CS-23 part.

- General Aviation (GA): Light aeroplanes supporting NCO operation, certified under CS-23 part.

4.2.2.1.2 Avionics characterisation

Avionics evolutions needed for operation in environments expected for the FAA NextGen program, and Single European Sky ATM Research (SESAR1) have been documented in SAE/IC ARINC 660B Report. This report referenced (in section 3) several avionics architecture and addressed the impacts of SESAR1 concepts on these airborne architectures (section 4). This characterisation was made according to aircraft's types' generations.

From avionics architecture generations presented as reference in ARINC 660B report, this section intents to summarise the main avionics architectural types -common to mainline, regional, and Bizet aircraft types- that are driving this solution deployment choices: federated avionics, and networked avionics. General aviation avionics is specific to the aircraft type and usually do not provide interface with aircraft systems (no aircraft data networking).

4.2.2.1.2.1 Federated avionics architecture

As shown in A660B, large aircraft types designed before and up to 1990's are based on a federated avionics. Insertion of the PP SWIM solution to these types should be addressed in term of avionics' retrofit.

Federated avionics architecture relies on an aircraft data networking function based on ARINC 429 DIGITAL INFORMATION TRANSFER SYSTEM (DITS) providing simplex data distribution. Duplex point to point exchange of data (at layer2) between LRUs required an additional protocol called general purpose bit oriented protocol (GPBOP) based on two generic A429 buses. Thus, federated aircraft data network was mainly a set of point to point data link between LRU equipment with a central routing device implementing the ARINC 618/619 ACARS routing function.

As such, introduction of an IP dedicated network (and associated devices) to such avionics would be, by nature, independent from the existing A429 based aircraft data network and equipment.

4.2.2.1.2.2 Networked avionics architecture

Networked avionics concepts were early implemented in some aircraft types designed in the 1990's and further refined in the 2000's and later certified aircraft. Insertion of the PP SWIM solution to these types should be either addressed in term of avionics' retrofit or forward fit.

Networked avionics architecture relies on a central aircraft data networking function based on ARINC 664 PART 7 AVIONICS FULL-DUPLEX SWITCHED ETHERNET NETWORK, complemented with specific point to point federated data link A429 buses.

Thus, safety critical avionics is connected via a certified bus, while other systems are connected via a standard (IP based) LAN. Cabin communication systems are fully separated and use dedicated media for air-ground connectivity, to ensure total segregation between aircraft data domains.

4.2.2.1.3 Avionics safety

SESAR Safety Process for Enablers-Technological Solutions (AF-GUI-01) targets a top down safety process from operational safety criteria, applied to technological enablers. However, as no CAT reference scenario is actually defined over PP SWIM solution, there are actually no FHA or safety objectives to rely on at this solution level.

Nevertheless, this section addresses avionics safety specificities (airplane airworthiness, and human factors in CAT operations), as described in §4.2.1.1, in order to assume minimal safety objectives to be considered while introducing SESAR PP AIR AG SWIM AP to aircraft systems, considering airplane airworthiness and human factors.

4.2.2.1.3.1 Airworthiness assessment

EASA CS 2x.1309 identified one of the main airworthiness requirements of embedded avionics system, as recall below:

> *"All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis"*

SAE ARP4754A is referenced as a mean of compliance to safety requirement, through the implementation of an adequate design assurance process.

As no safety criteria, objectives, or Functional Hazard Assessment (FHA) are available from operational solutions based PP SWIM solution, a full safety analysis process in compliance to SAE ARP4754A cannot be conducted in the solution timeframe.

However, a minimal strategy is possible at TRL6 level to ensure that compliance to EASA CS 2x.1309 is reachable when considering the integration of SESAR Air Purple Profile SWIM Node to aircraft systems.
Taking into account that avionics systems installed on aircrafts' holding a Type Certificate (TC) have already been recognised compliant to §1309 (either by ARP4754 Assurance level under POA, or by eTSO under A-DOA, approval), such safety objective s should be:

- Ensure that **any operational service**(s) intended to be **operated over the SESAR PJ17.01 SWIM Purple profile** have been **evaluated** by a reference authority **as having no safety effect** on civil air transport operations.
- Ensure that SESAR PJ17.01 **SWIM Purple profile integration to avionics system** does not adversely impact existing aircraft type certificate(s), by targeting a minimal impact installation that is not increasing avionics systems complexity, so that any required Supplemental type certification (STC) **only address minor changes**.

Minor avionics changes induce a minimal avionics architecture allowing an integration without major impact to Aircraft's initial configuration (e.g.: appliances), avionics interfaces (e.g.: aircraft domains and standardised interconnections), and existing avionics functionalities. This is addressed in §4.2.3.1, and §4.3.6.

4.2.2.1.3.2 Human factors assessment

EASA CS 2x.1302 identified main human factor requirements for embedded avionics system.

> *"Installed equipment must be shown, individually and in combination with other such equipment, to be designed so that qualified flight-crew members trained in its use can safely perform their tasks associated with its intended function."*

Air transport operations' human performance will not be evaluated against Air Purple Profile SWIM Node integration, as no CAT referenced concept of operation is actually defined by an operational solution. As a result, compliance to EASA CS 2x.1302 cannot be evaluated by this solution.

Yet, at a minimum, a procedure needs to be in place to prevent use of erroneous information by flight crews, and to ensure that operations over Air Purple Profile SWIM Node do not aversively impact the crew workload. In §4.3.6 a requirement about the impact of operations over Air Purple Profile SWIM Node on crew workload is provided. Requirements about procedures to prevent use of erroneous information by flight crews is out of scope of this solution because they concerns the application/SWIM layer (for all candidate Purple Profile enabled SWIM service a human factors assessment is needed).

4.2.2.1.4 Aircraft Data domain segregation

To reach Safety objectives, a key avionics principle relies on segregation to minimize exposure to hazards. Avionics data management is standardized against an Aircraft domain reference model. Aircraft domain reference model is specified in ARINC Report 664 P5 *Aircraft Data Network* which provides a notional model of the aircraft networking among the following four domains:

- Aircraft Control (AC) Domain
- Airlines Information Services (AIS) Domain
- Passenger Information and Entertainment Services (PIES) domain
- Passenger Owned Devices (PODs) domain

Resulting data domain segregation principles applicable to aircraft's data networking is documented in the ARINC Report 664 Part5 under "*Network domain characteristics and interconnection*", and detailed in ARINC Report 821 "Aircraft Network Server System (NSS) Functional definition" for the aircraft information systems capabilities, as recall below:

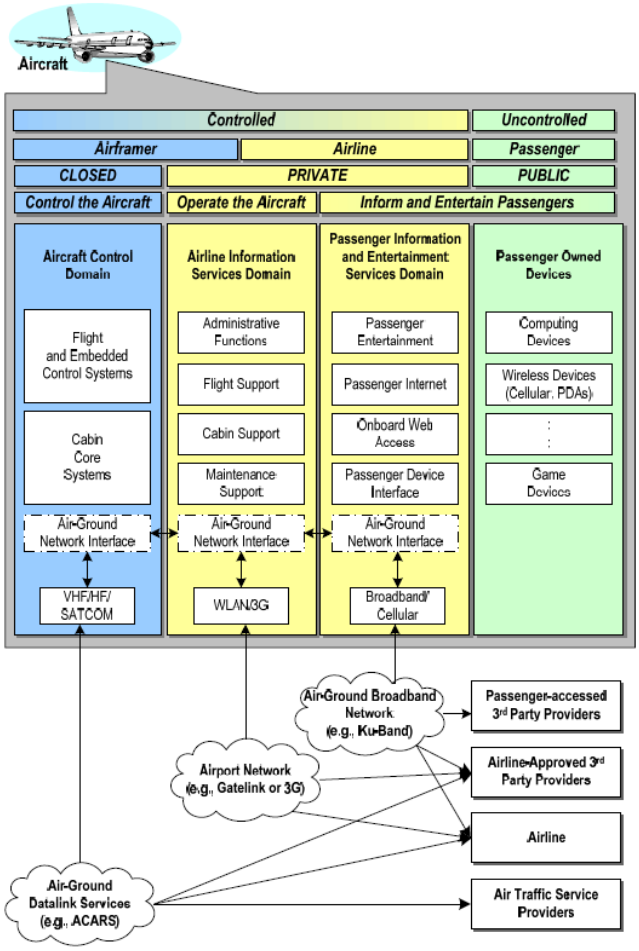


Figure 30: ARINC Report 821 Aircraft Network Services

Aircraft domains protection (Proper network configuration and domain isolation) is the responsibility of the aircraft systems integrator. Considering SESAR PJ17.01 solution target for "*non-safety aeronautical information services*", Air Purple Profile SWIM Node is part of an onboard information system, and thus belongs to the Airline Information Service Domain (AISD).

As consequences to this classification, integration of a PP AIR SWIM AP with avionics systems must respect the data domains segregation, and thus already approved (e.g.: qualified) data interfaces between aircraft data domains,

- Aircraft information domains must be physically kept segregated for safety and security reasons (advisory information belonging to Airline Information Services Domain).
- Aircraft networking is a shared resource that must be deterministic.
- Interface with Avionics ACD in order to access aircraft's parameters and data must be compliant with the standardised Aircraft Data Interface Function (ARINC 834 ADIF).

4.2.2.1.5 Aircraft Dispatch, Maintainability

Should a fault or failure of the system occur, it is essential that such failures are brought to the attention of the flight crew and that the system is isolated until rectification action is taken. In case of partial or complete failure of the system, alternative dispatch procedures should be followed. These procedures should be included either in the Minimum Equipment List (MEL) or in the Operations Manual to ensure an acceptable level of safety.

Aircraft maintenance and configuration control is operated under the Continuing Airworthiness Management Organisation (CAMO) regulation (Part M, Part 145), which is either regular scheduled (heavy, light …), or unscheduled (under GM1 MMEL.145 directives).

Considering SESAR PJ17.01 solution scope, Air Purple Profile SWIM Node

- Classification is either ATA 46-10 Airplane General Information Systems, or ATA 46-20 Flight Deck Information Systems,
- Its availability should fall under EASA EU-OPS GM1 ORO.MLR.105(a) for non-safety related equipment, assuming a "D" or below Rectification Interval Category (120 calendar days) considering Aircraft dispatch criteria.

Equipment configuration must be done on ground (under operator Part M or Part 145). Adequate test procedures are needed to ensure configured functionalities are operational, and Aircraft configuration must be maintained, as part of Continuous Airworthiness rules.

4.2.2.1.6 Avionics security

Aircraft information systems concerning domains security follows these guidelines:

> *Network security is the responsibility of the system integrator to meet airline/network service provider and must comply with airline security policy for remote operations and third-party information exchange.*

ARINC Report 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK provides guidance for developing such operational security concepts and provides an aircraft information security process framework, in addition with the following standardisation:

- A823 DATALINK SECURITY PART 2 – KEY MANAGEMENT,
- A842 GUIDANCE FOR USAGE OF DIGITAL CERTIFICATES,
- A852 GUIDANCE FOR SECURITY EVENT LOGGING IN AN IP ENVIRONMENT.

4.2.2.2 Messaging

In this section the Purple Profile messaging technical view is described. It aims at describing the "how" and "how good" concerning the messaging functions introduced in the functional view (§4.2.1.1).

In accordance with its SPA (A.1), the PP is explicitly targeted at:

- *High latency constraints and/or low bandwidth conditions.*
- *Need to minimize the communication overhead and the number of transport connections due to high cost of use of the communication.*

- *Intermittent and unpredictable availability of end-to-end connectivity over the communication infrastructure.*
- *Facilitate Security controls through constraints in the interaction patterns.*
- *Permanent need for time, space and synchronization decoupling between participants (asynchronous operations).*
- *Simple and easily certifiable information producers and consumers*.

Furthermore, only connection oriented technologies are allowed (i.e. no UDP) and *due to security reasons, ground-initiated communications to aircraft are forbidden. This means that the setup of a TCP session must always be initiated by the aircraft to prevent attacks from the ground* (Appendix A).

Above considerations represent the main design constraints for deriving the Purple Profile technical view from the functional view (Figure 28 and Figure 29).

4.2.2.2.1 Federated message exchange patterns

Permanent need for time, space and synchronization decoupling for all the Purple Profile technical use cases (Table 16) represents the main design constraint impacting the technical view of the messaging and in particular the message distribution function (related to MEPs).

All the MEPs and technical use cases (Table 16) are realized over asynchronous messaging-based distributed intermediary (refer to messaging characterization in Appendix B) aiming at decoupling aircraft and ground Purple Profile enabled applications in time, space and synchronization and dealing with additional constraints introduced above. This intermediary consists of interconnected and federated (SWIM-TI TAD §2.1.5, [51]) Air and Ground SWIM Nodes. The federated messaging entities (refer to messaging characterization in Appendix B) are Message Queue, Message Topic and Subscription handler.

The description of these mechanisms is provided in the sections below (for each MEP family). Table 24 provides, for each Purple Profile technical use case, the applicable MEP family (§3.1.1.2) and the link with Message Queue and Message Topic entities. Purple Profile allows only exclusive receiver: a given Message Queue can be consumed by one and only one receiver.

Furthermore, in Figure 31 the cardinality of the relationships between SWIM services, purple profile enabled applications and PP SWIM nodes is provided. It has to be noted that Air and Ground PP SWIM Nodes are entities introduced in the technical view without dealing with any deployment aspects: at this view no constraints are provided in terms of deployment (one or more hosts) and packaging of functions allocated to and provided by SWIM Nodes.

UC ID	UC Title	Aircraft role	Ground-based system role	Uplink / Downlink	MEP family	Information exchange cardinality	Information distribution mechanisms

PPUC-01a	Aircraft initiated Request/Response information exchange	Consumer	Provider	Uplink	Request/Response (or Request/Reply)	Many to one	Message Queue (For a given SWIM service N requestors to 1 responder with exclusive receivers)
PPUC-01b	Aircraft initiated Request/Multi-Response information exchange	Consumer	Provider	Uplink	Request/Response (or Request/Reply)	Many to one	Message Queue (For a given SWIM service N requestors to 1 responder with exclusive receivers)
PPUC-02	Ground-based system provided Publish/Subscribe information exchange	Consumer	Provider	Uplink	Publish/Subscribe	Many to many	Message Topic (For a given SWIM service N publishers to N subscribers)
PPUC-03a	Ground-based system initiated Request/Response information exchange	Provider	Consumer	Downlink	Request/Response (or Request/Reply)	Many to one	Message Queue (For a given SWIM service N requestors to 1 responder with exclusive receivers)
PPUC-03b	Ground-based system initiated Request/Multi-Response information exchange	Provider	Consumer	Downlink	Request/Response (or Request/Reply)	Many to one	Message Queue (For a given SWIM service N requestors to 1 responder with exclusive receivers)

PPUC-04	Aircraft provided Publish/Subscribe information exchange	Provider	Consumer	Downlink	Publish/Subscribe	Many to many	Message Topic (For a given SWIM service N publishers to N subscribers)

Table 24: SWIM Purple Profile technical use cases and information distribution mechanisms

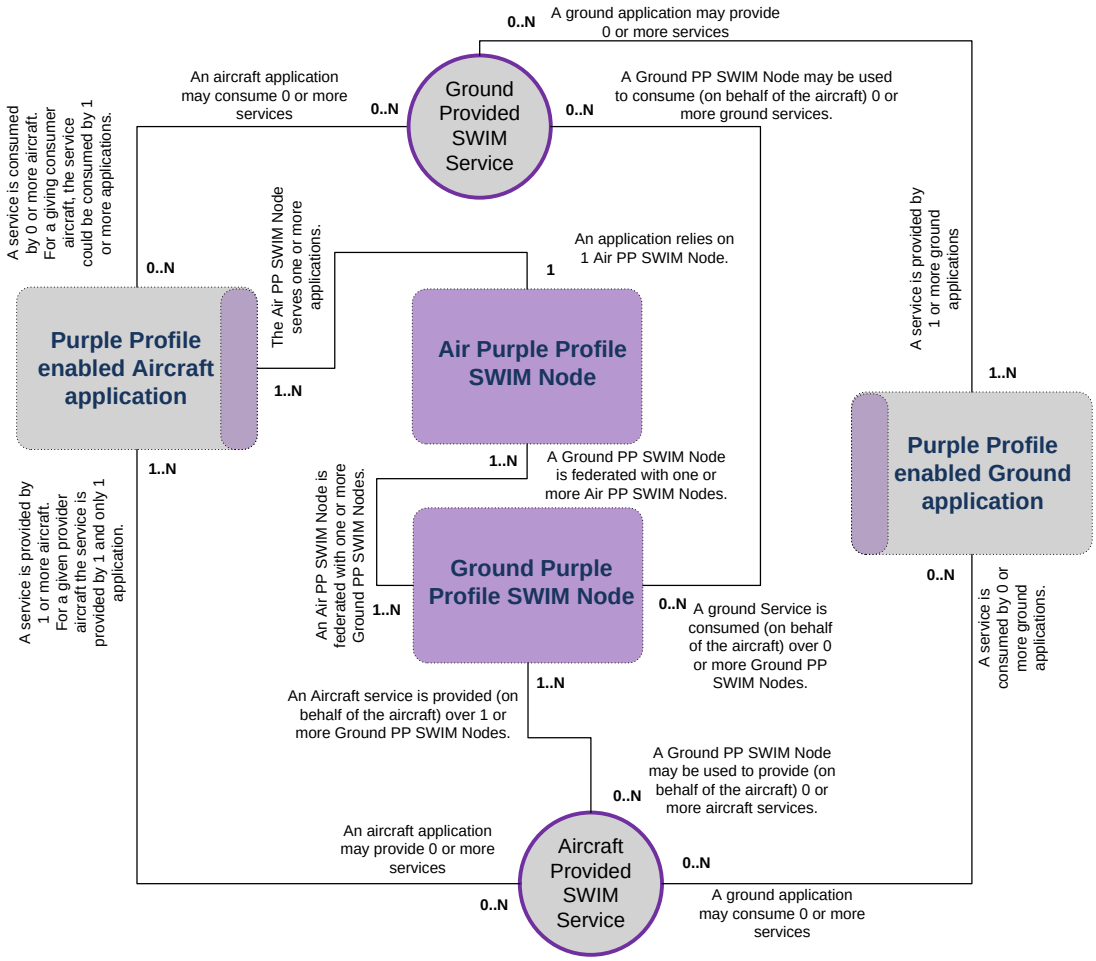


Figure 31: Purple Profile technical view – cardinality of the relationships between main entities

Ground-based systems interacting with aircraft may use different protocol stacks, MEPs and data representation with respect to those adopted by the Purple Profile interface bindings. Therefore, up to three distinct forms of transformation may be needed:

- Protocol stack transformation (protocol bridging) up to and including the messaging protocol (e.g. between an AMQP based stack and a SOAP based stack).
- Data format transformation (e.g. between ASN.1 and XML).

- MEP transformation: between synchronization decoupled MEP and a synchronization coupled MEP.

The Purple Profile messaging infrastructure does not provide any “bridging” capabilities related to the adaptation towards ground Profiles (Yellow, Blue, Green, etc.). This is mainly to avoid coupling between SWIM Profiles and because of the complexity of a complete bridging for all the existing interface bindings. This decision is based on following assumptions:

- Ground provided services of interest for the aircraft are provided over Purple Profile <Service binding> options specified in this technical specification.
- Ground provided services of interest for both the aircraft and ground systems are provided over multiple SWIM Profiles.

Ground applications are said Purple Profile enabled when they are able to:

- provide ground Purple Profile enabled SWIM service according to Purple Profile defined <Service binding>.
- consume aircraft Purple Profile enabled SWIM service according to Purple Profile defined <Service binding>.

Similar adaptation/integration needs can be envisaged also on the aircraft side. Also in this case, these needs are allocated to an external to PP component : Aircraft Server. The main purpose of this technical component is to support adaptability to avionics architecture (protocol bridge and data transformation messaging capabilities introduced above). Furthermore, this component is responsible for:

- Managing on one hand a local interface with the Air Purple Profile Messaging and, on the other hand, providing messaging resources to aircraft applications for exchanging messages to/from that interface (e.g. messages from the aircraft Purple Profile Messaging are then made available to aircraft applications).
- Handling persistent subscriptions, dynamic updates, and request to response associations.
- User preferences management and avionics dependent maintainability functions.
- Managing interface(s) with aircraft applications.

This component is part of the overall aircraft architecture and this specification does not provide any:

- technical requirements concerning the interfacing layer between this component and the aircraft technical systems/aircraft applications.
- Functional or technical requirements for this component.

Aircraft application are said Purple Profile enabled when they are able to:

- provide aircraft Purple Profile enabled SWIM service according to Purple Profile defined <Service binding>.
- consume ground Purple Profile enabled SWIM service according to Purple Profile defined <Service binding>.

The Aircraft Server is an optional aircraft architecture component enabling aircraft applications to be Purple Profile enabled.

4.2.2.2.1.1 Request/Response

For simplicity the analysis refers to PPUC-01 and PPUC-03 without distinguishing between the use case based on FDRR-MEP (PPUC-01a and PPUC-03a) and those based on FDRMR-MEP (PPUC-01b and PPUC-03b). The latter is a generalization of the FDRR-MEP where multiple responses are exchanged.

Information exchange based on this MEP are conceptually relying on two functions:

- Message Distribution which deals with the delivery of the request and response messages.
- Administration which deals with the management aspects such as configuration and monitoring.

Administration needs (configuration) are described in §4.2.2.5 where the concerning interface bindings are described. Monitoring needs are addressed as part of reliability and performance efficiency requirements.

In Figure 32 the conceptual view for both PPUC-01 and PPUC-03 is provided. The use cases consist of a ground/aircraft provided SWIM service consumed by several ground/aircraft-based consumers.

Each requestor sends the Request Message to the Request Message Queue for that specific service. The responder (or replier) processes the request and replies with a Response Message sent to a Response Message Queue. In Figure 32 two key concepts adopted in this kind of interaction are depicted: “reply-to” (or “Return address”) and message “correlation”.

The “reply-to” allows the requestor to specify the Response Message Queue the responder has to use when sending the Response Message. This eliminates the need for the responder to “know” that information in advance. This concept is realized by adding the Response Message Queue information to the header/metadata of the Request Message.

The message “correlation” allows the requestor to discover which Request Message a received Response Message relates to. This is realized by adding a message identifier in the header/metadata of the Request Message and using the same value as correlation identifier in the header/metadata of the Response Message for that request.

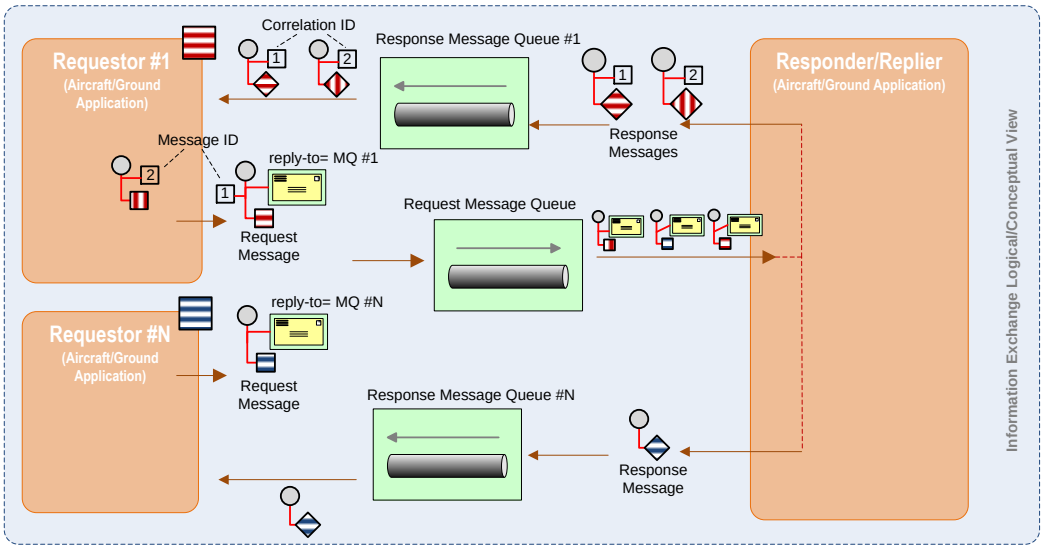


Figure 32: PPUC-01 and PPUC-03 (Request/Response) conceptual view

In Figure 33 both functional and technical views of the PPUC-01 use case are depicted:

- The federation of the request message queue (functional view) mainly consists in message routing and between triad of message queues (technical view):
    - Air side message queue (Air PP SWIM Node messaging resource) allows one or more aircraft applications to send request for that service in a time, space and synchronization decoupled manner. For each SWIM service over the PPUC-01 a dedicated message queue is available and it is federated with one message queue on Ground PP SWIM Node side (consumption of different SWIM services over the PPUC-01 could occur via different Ground SWIM Nodes). The federated Ground SWIM Node could be then replicated as described in the context of reliability design.
    - Ground PP SWIM Node side request message queue allows federation of air side request message queues from one or more aircraft. Depending on segregation/QoS needs, for each SWIM service over the PPUC-01 is it possible to configure a dedicated message queue or one shared for all/a group of SWIM services.
    - Ground side request message queue allows ground applications to receive request messages for that service. This is a messaging resource part of the service provider messaging.
- The federation of the response message queue (functional view) mainly consists in message routing and between triad of message queues (technical view):
    - Ground side response message queue allows Ground PP SWIM Node to receive response messages for that service. This is a messaging resource that could be part of the service provider or Ground PP SWIM Node messaging.
    - Ground PP SWIM Node side response message queues allows federation of air side response message queues to one or more aircraft. For each federated aircraft (Air SWIM Node) a dedicated response message queue is allocated. This queue is used to route response messages concerning all requestor applications on-board of that aircraft. Depending on segregation/QoS needs, for each SWIM service over the PPUC-01 is it possible to configure a dedicated response message queue or one shared for all/a group of SWIM services.
    - Air side response message queues (Air PP SWIM Node messaging resource) allows one or more aircraft applications to receive response messages concerning requests they sent. For each requestor application a dedicated response message queue is allocated.

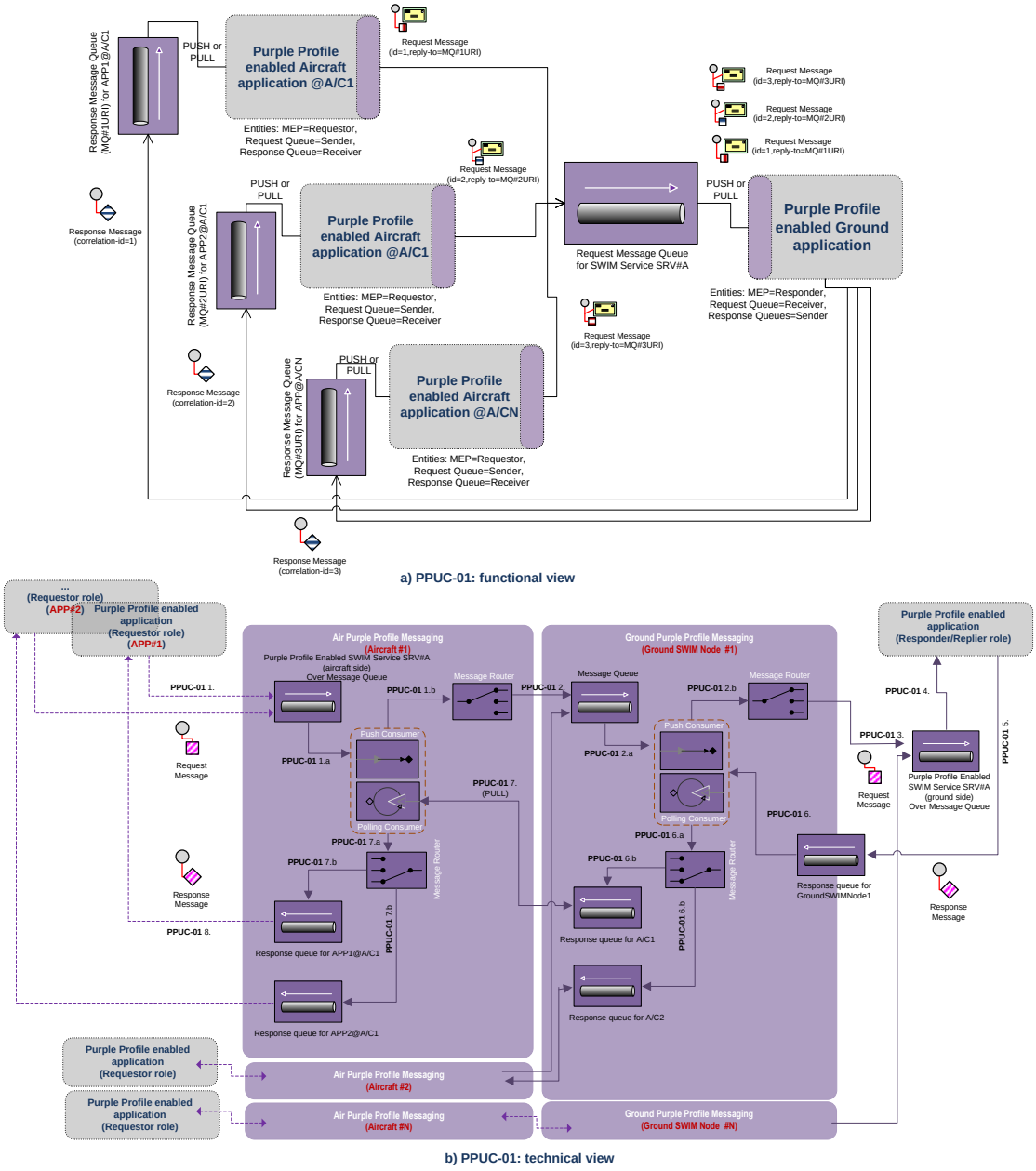


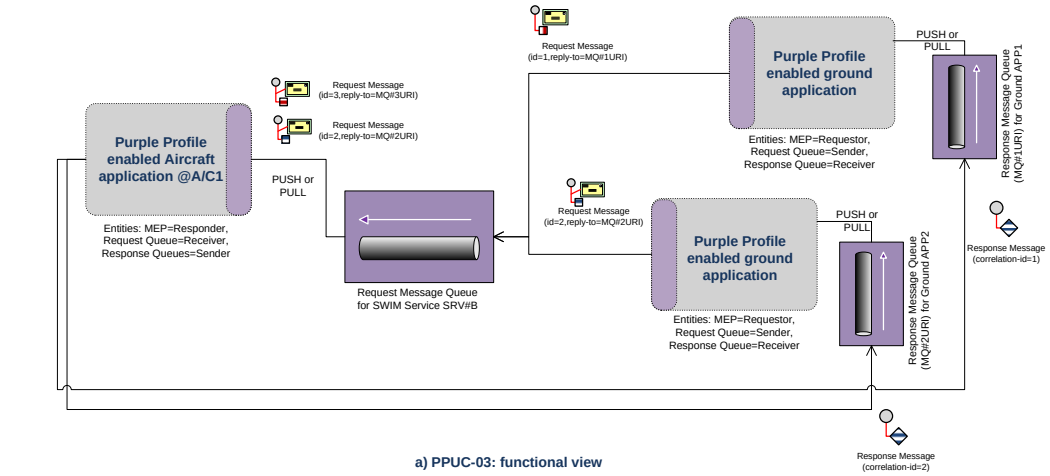
Figure 33: Purple Profile PPUC-01 technical view

In Figure 34 both functional and technical views of the PPUC-03 use case are depicted:

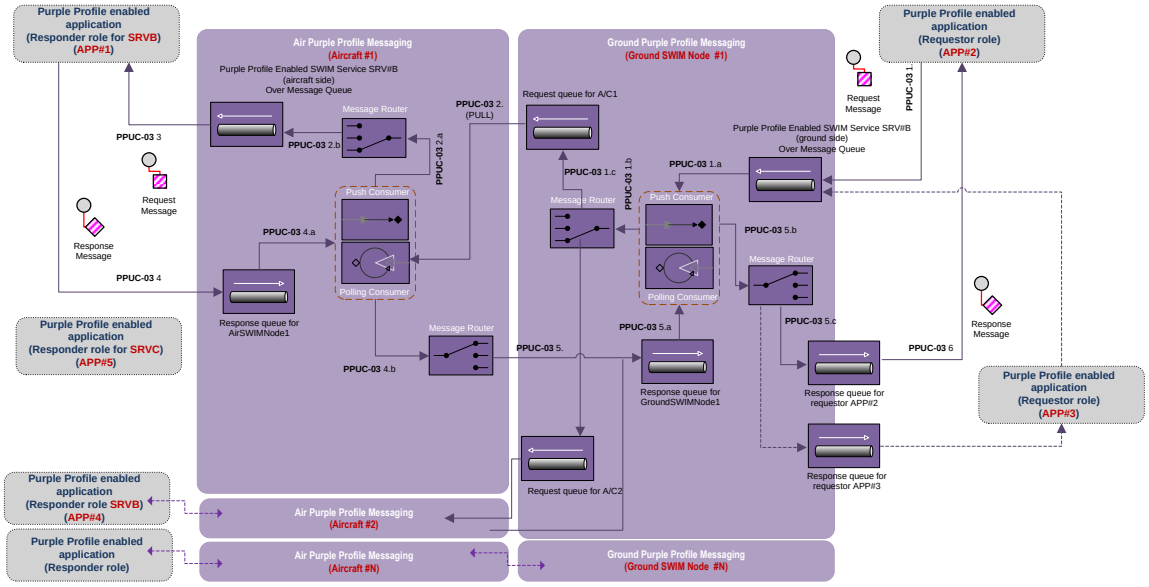
- The federation of the request message queue (functional view) mainly consists in message routing and between triad of message queues (technical view):
  - Ground side message queue (Ground PP SWIM Node messaging resource) allows one or more ground applications to send request for that service in a time, space and synchronization decoupled manner. For each SWIM service over the PPUC-03 a dedicated message queue is available.

- Ground PP SWIM Node side request message queue allows federation of air side request message queues from one or more aircraft. Depending on the design of the SWIM service, it could happen that more than one responders are available. As part of the request message routing the target requestor (request queue ground side) is identified (in the figure both A/C1 and A/C2 play the responder role for that service). Furthermore, depending on segregation/QoS needs, for each SWIM service over the PPUC-03 is it possible to configure a dedicated message queue or one shared for all/a group of SWIM services (e.g. “Request queue for A/C1” in figure could be used to route request messages concerning different SWIM services).
- Air side request message queue allows aircraft applications to receive request messages for that service.

- The federation of the response message queue (functional view) mainly consists in message routing and between triad of message queues (technical view):
  - Air side response message queue (Air PP SWIM Node messaging resource) allows one or more aircraft applications to send response messages in a time, space and synchronization decoupled manner. For each SWIM service over the PPUC-03 a dedicated or shared message queue is available.
  - Ground PP SWIM Node side response message queue allows federation of air side response message queues from one or more aircraft. Depending on segregation/QoS needs, for each SWIM service over the PPUC-03 is it possible to configure a dedicated message queue or one shared for all/a group of SWIM services.
  - Ground side response message queue allows ground applications to receive response messages. This is a messaging resource that could be part of the requestor or Ground PP SWIM Node messaging.



a) PPUC-03: functional view



b) PPUC-03: technical view

Figure 34: Purple Profile PPUC-03 technical view

The mapping of publication message and subscription management messages onto AMQP and PP specific constraints are provided in §4.2.2.5 where the interface bindings are described.

4.2.2.2.1.2 Publish/Subscribe

Information exchange based on Publish/Subscribe MEPs are based on four functions:

- Subscription Management which deals with the life cycle of the interest that a subscriber expresses to be informed about particular publications or not.
- Publication Registration Management which deals with the life cycle of the interest that a publisher expresses to perform particular publications
- Message Distribution which deals with the delivery of the messages that contain the publications from the publisher to the publication consumers (PSPUSH-MEP and PSPULL-MEP).

- Administration which deals with the management aspects such as configuration and monitoring.

Administration needs (configuration) are described in §4.2.2.5 where the concerning interface bindings are described. Monitoring needs are addressed as part of reliability and performance efficiency requirements.

Publication Registration Management is useful when multiple publishers write to the same Message Topic. Publishers registration enables a number of capabilities such as message filtering based on the message publisher, message enrichment by adding publisher identifier, publisher lifecycle management and monitoring, etc. In the context of the Purple Profile this function is considered applicable. In particular:

- PPUC-02: multiple ground Publishers may publish messages to the same Message Topic.
- PPUC-04: multiple aircraft Publishers may publish messages to the same Message Topic.

Currently no interoperability needs have been envisaged for a dynamic Publication Registration Management function: when needed, this function is realized via off-line exchange (e.g. SLA agreement and configuration) and not over <Service binding>.

In Figure 35 both functional and technical views of the PPUC-02 use case are depicted:

- The federation of the message topic (functional view) mainly consists in message routing and filtering between triad of message topics (technical view):
    - Air side message topic (Air PP SWIM Node messaging resource) allows one or more aircraft applications to consume that service in a time, space and synchronization decoupled manner. For each SWIM service over the PPUC-02 a dedicated message topic is available and it is federated with one message topic on Ground PP SWIM Node side (consumption of different SWIM services over the PPUC-02 could occur via different Ground SWIM Nodes). The federated Ground SWIM Node could be then replicated as described in the context of reliability design.
    - Ground PP SWIM Node side message topic allows federation of air side message topics from one or more aircraft (cardinality of publication message is many to many). Depending on segregation/QoS needs, for each SWIM service over the PPUC-02 is it possible to configure a dedicated message topic or one shared for all/a group of SWIM services. The Ground PP SWIM Node is responsible for properly handling the case where two different aircraft applications on-board on the same aircraft require different subscription time filtering criteria.
    - Ground side message topic allows ground applications to publish messages for that service. This is a messaging resource part of the service provider messaging.
- The federation of the subscription handler (functional view) mainly consists in message routing between triad of subscription handlers (technical view).
    - Air side the subscription handler (Air PP SWIM Node messaging resource) is responsible for routing subscription management messages and maintaining subscription status information. This subscription handler is able to handle subscription management for all the SWIM service over the PPUC-02.
    - Ground PP SWIM Node side subscription handler is responsible for routing subscription management messages and maintaining subscription status

information. This subscription handler is able to handle subscription management for all the SWIM service over the PPUC-02 consumed via that Ground SWIM Node.

- Ground side subscription handler is responsible for the actual handling of subscription management messages (e.g. accept subscription request) and maintaining active subscriptions. This is a messaging resource part of the service provider messaging.

This specification provides the definition of the subscription management messages (XML schema). The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services described in §4.2.2.2.1.1 (the responder is the subscription handler responsible for accepting or not the subscription management request messages).

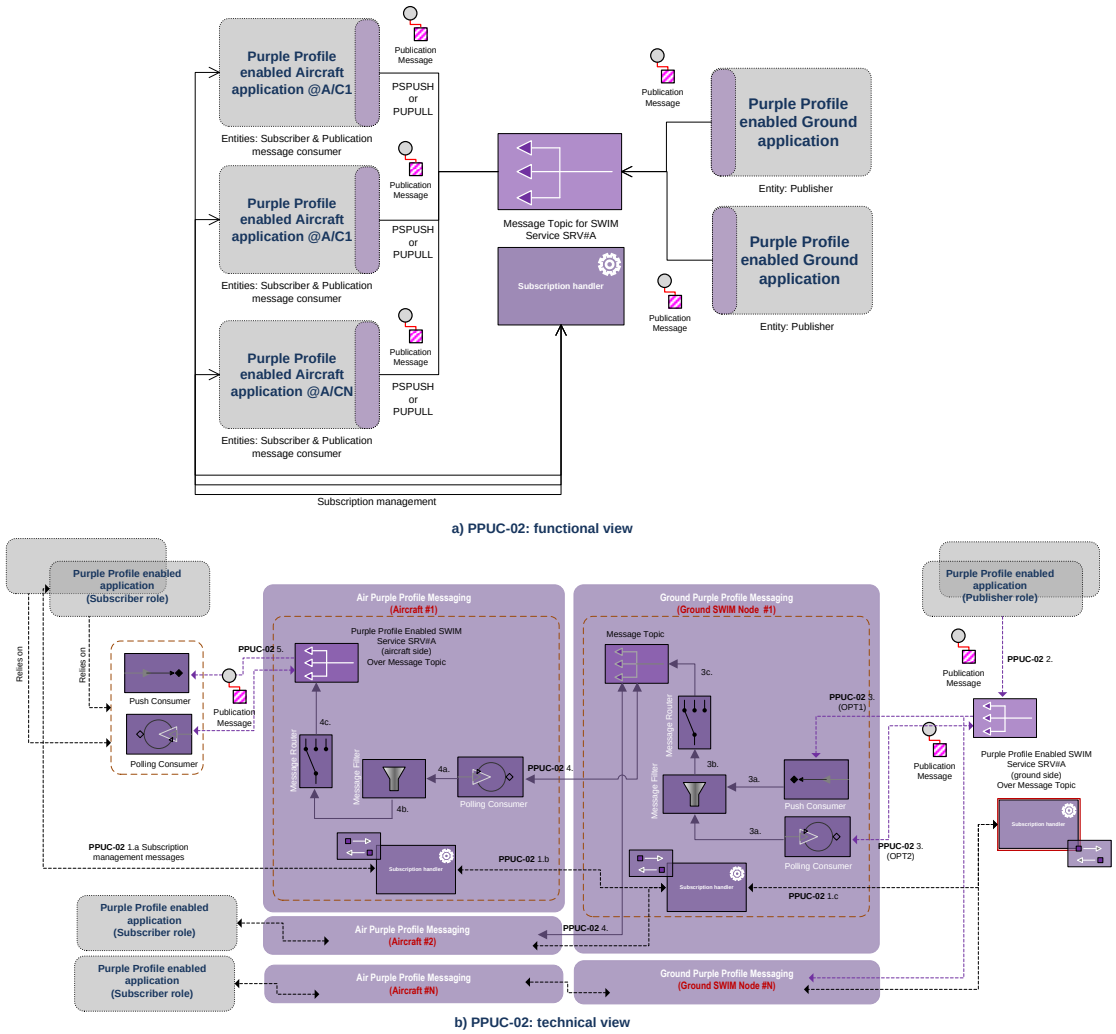


Figure 35: Purple Profile PPUC-02 technical view

In Figure 36 both functional and technical views of the PPUC-04 use case are depicted:

- The federation of the message topic (functional view) mainly consists in message routing and filtering between triad of message resources (technical view):
    - Air side message topic (Air PP SWIM Node messaging resource) allows the aircraft application to publish messages for that service in a time, space and synchronization decoupled manner. For each SWIM service over the PPUC-04 a dedicated message topic is available and it is federated with one message queue on Ground PP SWIM Node side (provisioning of different SWIM services over the PPUC-04 occurs via the same Ground SWIM Nodes). The federated Ground SWIM Node could be then replicated as described in the context of reliability design.
    - Ground PP SWIM Node side message queue allows federation of air side message topics from one or more aircraft (cardinality of publication message between aircraft and Ground SWIM Node is many to one). Depending on segregation/QoS needs, for each SWIM service over the PPUC-04 is it possible to configure a dedicated message queue or one shared for all/a group of SWIM services.
    - Ground PP SWIM Node side message topic allows ground applications to consume messages for that service published by one or more aircraft.
- The federation of the subscription handler (functional view) mainly consists in message routing between subscription handlers (technical view) in a similar way described for PPUC-02. The main specificities for the PPUC-04 are the following:
    - More than one aircraft could play the publisher role: which subscription handler is actually accepting/rejecting the subscription management messages?
        - All the subscription handlers on-board of the publishing aircraft: this requires response message aggregation/grouping with complex logics when (e.g.) only some aircraft accept the request.
        - Only the subscription handler on the Ground PP SWIM Node side: active subscriptions are not visible to publishing aircraft. This means that the aircraft could continue publishing even if there are no active subscriptions (durable or not) and this implies a useless consumption of Air/ground network resources.
    - The design decision is to adopt the following solution representing the right trade-off between the two cases above:
        - It is up to the subscription handler on the Ground PP SWIM Node side to handle subscription management messages but it is also responsible to inform concerned subscription handlers on-board of the publishing aircraft about relevant subscription management events.
        - The subscription handlers on-board of the publishing aircraft are not responsible for accepting/rejecting the subscription management messages but they have to make sure that messages are published according to active subscriptions.
    - It has to be noted that it could happen that aircraft application on-board of the publishing aircraft may be interested in published information. In this case, the subscription handler on-board of that aircraft is responsible for accepting or not the subscription request (no interaction with the ground are required).

Company General Use

This specification provides the definition of the subscription management messages (XML schema). The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services described in §4.2.2.2.1.1 (the responder is the subscription handler responsible for accepting or not the subscription management request messages).

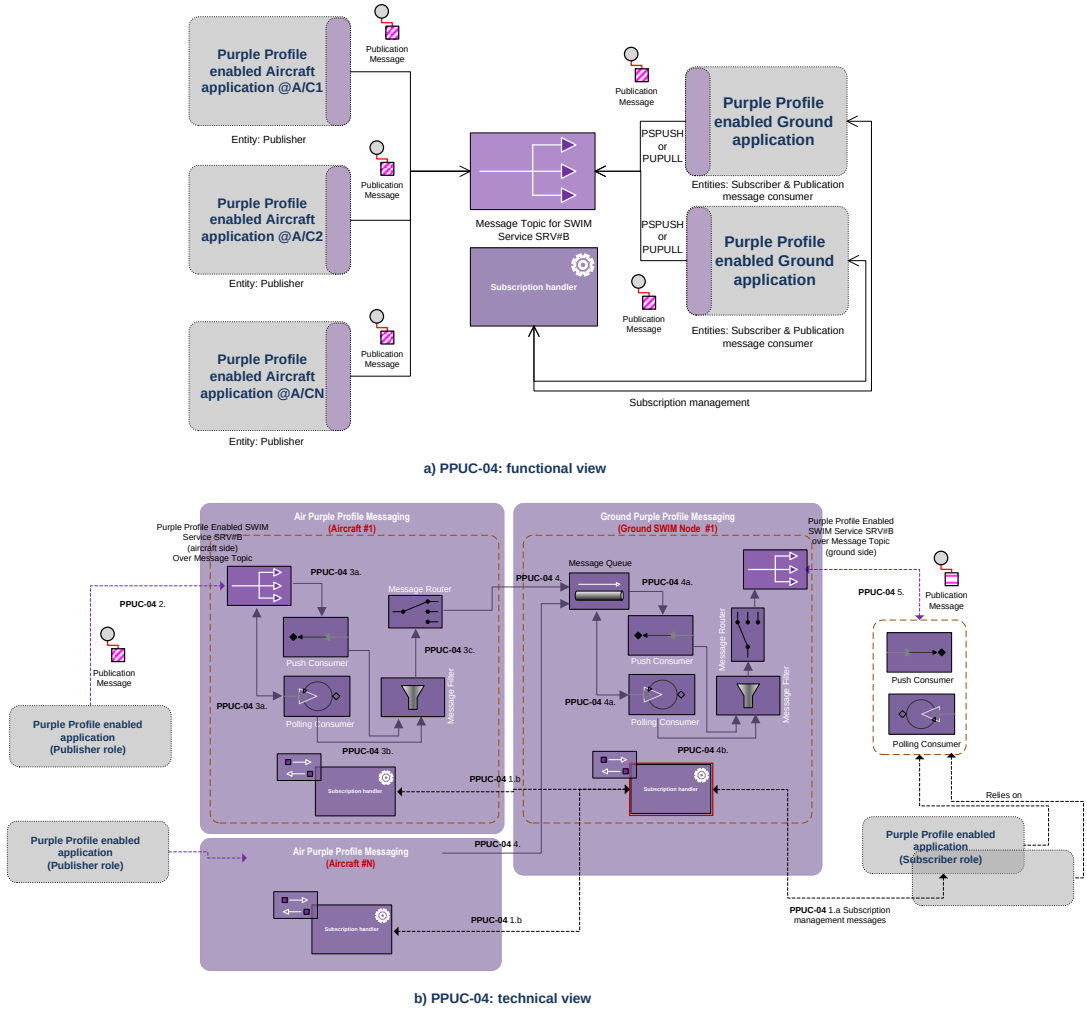


Figure 36: Purple Profile PPUC-04 technical view

The mapping of publication message and subscription management messages onto AMQP and PP specific constraints are provided in §4.2.2.5 where the interface bindings are described. In the remaining part of this section a table-based description of the data elements concerning subscription management messages is provide. Based on these data elements, the subscription management XSD has been defined and it is available in the Appendix D.

Following pairs of subscription management messages have been identified:

- *SubscriptionRequest* and *SubscriptionResponse*: subscription request operation allows applications to indicate the interest in receiving publication messages concerning a given

SWIM service over Publish/Subscribe. This operation is provided and handled by the subscription handlers described above.

- *UnsubscriptionRequest* and *UnsubscriptionResponse*: unsubscription request operation allows applications to terminate active subscriptions. This operation is provided and handled by the subscription handlers described above.
- (advanced and not part of the <PP Core>) *SubscriptionRenewRequest* and *SubscriptionRenewResponse*: active subscription renewal allows applications to renew active subscriptions. This operation is provided and handled by the subscription handlers described above.
- (advanced and not part of the <PP Core>) *UpdateSubscriptionFilterRequest* and *UpdateSubscriptionFilterResponse*: this request message allows applications to update the filtering criteria (if any) provided at subscription time. This is not applicable to *Topic Expression* (Table 26) and *Producer Properties Selector* (Table 26): it is restricted only to *Message Content Selector* (Table 26). This operation is provided and handled by the subscription handlers described above.
- *ActiveSubscriptionsRequest* and *ActiveSubscriptionsResponse*: active subscriptions retrieving operation allows applications to retrieve their active subscriptions. This operation is provided by aircraft and ground subscription handlers. It does not require specific message flow (federation logics) between aircraft and ground messaging; it is realized by relying on local (aircraft or ground) information concerning active subscriptions.
- (advanced and not part of the <PP Core>) *ActiveSubscriptionsNotify*: as anticipated above, for downlink Publish/Subscribe services, It is up to the subscription handler on the Ground PP SWIM Node side to handle subscription management messages but it is also responsible to inform concerned subscription handlers on-board of the publishing aircraft about relevant subscription management events. The subscription handlers on-board of the publishing aircraft are not responsible for accepting/rejecting the subscription management messages but they have to make sure that messages are published according to active subscriptions. The ActiveSubscriptionsNotify message (one-way, no responses are required) is the message used by the subscription handler on the Ground PP SWIM Node side to notify concerned Air side subscription handlers. This message can be sent periodically or triggered by subscription updates (e.g. unsubscription, subscription renew, etc.).

In Table 25 the description of the SubscriptionRequest message is provided.

Element name	Type	Description	Note
Consumer Queue reference	MessageQueueAddressType	Optional element. Consumer provided address of the Message Queue to which the publication messages have to be sent to. When not provided by the subscribing entity, the consumer queue reference shall be retuned in the SubscriptionResponse upon	The actual type in the XSD is “xsd:anyURI”.

		subscription request accepted.	
Filter	FilterType	Mandatory element. Consumer provided one or more filtering criteria to apply subject based filtering.	The type is further detailed in the tables below.
Subscription Policy	SubscriptionPolicy	Optional element. Consumer provided Subscription Policy aiming to specify Quality of Services at subscription level and additional NFRs such as message rate.	The XSD includes a generic type (generic HashMap) for further or service specific policies. Currently only one PP specific policy has been defined: subscription with fixed termination time (hash map key must be "FixedTerminationTime").
Consumer Identifier	Name-Based UUID (RFC 4122)	The Name-based UUID of the actual application layer entity subscribing to the Message Topic.	This solution will define conventions used for allocating names and ensuring their uniqueness within the Purple Profile name spaces. The namespaces are actually expected to be created and handled at technical validation exercise level. Possible approach could be to assign names based on application/service name + X.500 Distinguished Names (DNs) from X.509 certificates used at interface binding level. It is assumed that when moving to the SESAR deployment phase, a governed registry will be available to register applications, services, etc.

Table 25: Purple Profile Subscription Request Message

In the table below the *FilterType* type is described.

Element name	Type	Description	Note
Topic Expression	URI (RFC3986)	Mandatory and it has to be evaluated in AND condition with all the other filtering criteria. This is the URI of the Message Topic of interest. This element is used to realize subject based filtering based on the topic URI.	The actual type in the XSD is "xsd:anyURI".
Message Content Selector	LengthRestrictedString	Optional and when provided it has to be evaluated in AND condition with all the other filtering criteria. This element is used to realize subject based	

		filtering based on message properties. Message selector with semantics and syntax in accordance to JMS 2.0 "*Message Selector*".	
Producer Properties Selector	LengthRestrictedString	Optional and when provided it has to be evaluated in AND condition with all the other filtering criteria. Message selector with semantics and syntax in accordance to JMS 2.0 "*Message Selector*". Even if the same behaviour can be realized by adding producer specific properties and applying the Message Content filter, it is recommended to keep separated the filtering on producers properties separated because of their relevance.	

Table 26: Purple Profile Subscription Request Message - Filter type

In Table 27 the description of the Fixed termination time subscription policy is provided. One and only one of the two elements is allowed (xsd:choice). When this policy is not provided the subscription is not expected to expire.

Element name	Type	Description	Note
Absolute termination time	Date and time	Absolute time when the subscription is expected to expire. Policies with this value not in the future shall be rejected.	The actual type in the XSD is "xsd:dateTime".
Duration	Duration	Absolute time when the subscription is expected to expire is calculated by adding the provided duration to the current time of the subscription handler.	The actual type in the XSD is "xsd:duration".

Table 27: Purple Profile Fixed termination time subscription policy

In Table 28 the description of the SubscriptionResponse message is provided. The message will include one and only one of the two elements (xsd:choice)

Element name	Type	Description	Note
Subscription Reference	SubscriptionReferenceType	The subscription reference in case the subscription is accepted.	The type is further detailed in the tables below.
Subscription Processing Fault	**SubscriptionFaultType**	Composite type containing the enumeration of faults associated with failure to process the subscription request message and a string (free text) containing additional information about the fault (e.g. which filter is not supported).	The identified fault are described in the table below. The XSD has been designed for extensibility meaning that in addition to identified faults additional ones could be provided.

Table 28: Purple Profile Subscription Response Message

Element name	Type	Description	Note
Subscription Identifier	Random UUID variant 2 version 4 (RFC 4122)	Mandatory element. The UUID of the accepted subscription.	
Consumer Queue reference	MessageQueueAddressType	Mandatory element. Address of the Message Queue to which the publication messages have to be sent to.	
Absolute termination time	Date and time	Optional and in response to Fixed termination time subscription policy. It represents the absolute time when the subscription is will expire.	

Table 29: Purple Profile Subscription Response Message - SubscriptionReferenceType

Enumeration	Description	Note
TopicNotSupported	The subscription message refers to a Message Topic not supported or unknown.	
FilterNotSupported	The subscription message contains a Filter not supported or unknown.	
InvalidFilter	The subscription message contains a Filter that is evaluated as invalid.	
SubscriptionPolicyNotSupported	The subscription message contains a Subscription Policy that is not supported.	This applies also in the case when the subscription handler does not support (it is an advanced feature) the Fixed termination time subscription policy.
InvalidSubscriptionPolicy	One or more subscription policies are not valid.	
SubscriptionAlreadyExists	The subscribing application is already subscribed to the target Message Topic.	
MalformedRequest	The request is not syntactically valid against the reference XML schema (payload) and properties.	
InfrastructureFault	An error occurred at infrastructure level.	
NoXMLContentType	No content type property is available in the AMQP message or when it is not “application/xml”.	
NoMessageID	The AMQP message does not contain the messageid.	
InvalidMessageType	The provided subject is null or unknown.	
NoReplyTo	The request AMQP message does not contain the reply-to.	
DigitalSignatureValidationFault	The Digital signature in not available or not valid.	

Table 30: Purple Profile Subscription Response Message – SubscriptionFault enumeration

The unsubscription request and response messages are described in the tables below.

Element name	Type	Description	Note
Subscription Reference	SubscriptionReferenceType	The Subscription Reference provided as response message to subscription request.	

Table 31: Purple Profile Unsubscription Request Message

In Table 32 the description of the UnsubscriptionResponse message is provided. The message will include one and only one of the two elements (xsd:choice)

Element name	Type	Description	Note
Subscription Reference	SubscriptionReferenceType	The Subscription Reference identifying the subscription successfully terminated.	
Unsubscription Processing Fault	**UnsubscriptionFaultType**	Composite type containing the enumeration of faults associated with failure to process the unsubscription request message and a string (free text) containing additional information about the fault (e.g. which filter is not supported).	The identified fault are described in the table below. The XSD has been designed for extensibility meaning that in addition to identified faults additional ones could be provided.

Table 32: Purple Profile Unsubscription Response Message

Enumeration	Description	Note
UnknownSubscription Reference	The provided Subscription Reference is not known (no active subscription linked to that Subscription Reference)	
MalformedRequest	The request is not syntactically valid against the reference XML schema (payload) and properties.	
InfrastructureFault	An error occurred at infrastructure level.	
NoXMLContentType	No content type property is available in the AMQP message or when it is not “application/xml”.	
NoMessageID	The AMQP message does not contain the messageid.	
InvalidMessageType	The provided subject is null or unknown.	
NoReplyTo	The request AMQP message does not contain the reply-to.	
DigitalSignatureValidationFault	The Digital signature in not available or not valid.	

Table 33: Purple Profile Unsubscription Response Message – UnsubscriptionFault enumeration

In the tables below the description of the data element composing the active subscriptions request and response messages is provided.

Element name	Type	Description	Note
Consumer Identifier	Name-Based UUID (RFC 4122)	*Consumer Identifier* identifying the entity for which the active subscriptions have to be retrieved. This identifier must be the same used in the subscription request.	This solution will define conventions used for allocating names and ensuring their uniqueness within the Purple Profile name spaces. The namespaces are actually expected to be created and handled at technical validation exercise level. Possible approach could be to assign names based on application/service name + X.500 Distinguished Names (DNs) from X.509 certificates used at interface binding level. It is assumed that when moving to the SESAR deployment phase, a governed registry will be available to register applications, services, etc.

Table 34: Purple Profile Active Subscriptions Request Message

In Table 35 the description of the ActiveSubscriptionResponse message is provided. The message will include one and only one of the two elements (xsd:choice)

Element name	Type	Description	Note
Active Subscriptions	Collection of *SubscriptionType*	A collection of the active subscriptions of the entity identified in the Active Subscription request message. Empty in case there are no active subscriptions for that entity.	SubscriptionType is further detailed in the table below.
Active Subscriptions Processing Fault	ActiveSubscriptionsProcessingFaultType	Composite type containing the enumeration of faults associated with failure to process the active subscription request message and a string (free text) containing additional information about the fault (e.g. which filter is not supported).	The identified fault are described in the table below. The XSD has been designed for extensibility meaning that in addition to identified faults additional ones could be provided.

Table 35: Purple Profile Active Subscriptions Response Message

Element name	Type	Description	Note
SubscriptionReference	SubscriptionReferenceType		
Filter	FilterType		
SubscriptionPolicy	SubscriptionPolicy	Optional element.	

Table 36: Purple Profile Active Subscriptions Response Message - SubscriptionType

Enumeration	Description	Note
MalformedRequest	The request is not syntactically valid against the reference XML schema (payload) and properties.	
InfrastructureFault	An error occurred at infrastructure level.	
NoXMLContentType	No content type property is available in the AMQP message or when it is not “application/xml”.	
NoMessageID	The AMQP message does not contain the messageid.	
InvalidMessageType	The provided subject is null or unknown.	
NoReplyTo	The request AMQP message does not contain the reply-to.	
DigitalSignatureValidationFault	The Digital signature in not available or not valid.	

Table 37: Purple Profile Active Subscriptions Response Message – ActiveSubscriptionsProcessingFault enumeration

The SubscriptionRenewRequest and SubscriptionRenewResponse messages are described in the tables below.

Element name	Type	Description	Note
Subscription Reference	SubscriptionReferenceType	The Subscription Reference provided as response message to subscription request.	
Termination time	Absolute termination time	Absolute time when the subscription is expected to expire. Policies with this value not in the future shall be rejected. The actual type in the XSD is “xsd:dateTime”.	With xsd:choice semantics
	Duration	Absolute time when the subscription is expected to expire is calculated by adding the provided duration to the current time of the subscription handler. The actual type in the XSD	

		is “xsd:duration”.	

Table 38: Purple Profile Subscription Renew Request Message

In Table 39 the description of the SubscriptionRenewResponse message is provided. The message will include one and only one of the two elements (xsd:choice)

Element name	Type	Description	Note
Subscription Reference	**SubscriptionReferenceType**	The Subscription Reference identifying the subscription successfully renewed. It includes the new termination time.	
Subscription Renew Processing Fault	**SubscriptionRenewFaultType**	Composite type containing the enumeration of faults associated with failure to process the subscription renew request message and a string (free text) containing additional information about the fault.	The identified fault are described in the table below. The XSD has been designed for extensibility meaning that in addition to identified faults additional ones could be provided.

Table 39: Purple Profile Subscription Renew Response Message

Enumeration	Description	Note
UnknownSubscription Reference	The provided Subscription Reference is not known (no active subscription linked to that Subscription Reference)	
SubscriptionPolicyNotSupported	The Subscription Policy is not supported (i.e. subscription renew is not supported).	
InvalidTerminationTime	The provided termination time is not in the future.	
MalformedRequest	The request is not syntactically valid against the reference XML schema (payload) and properties.	
InfrastructureFault	An error occurred at infrastructure level.	
NoXMLContentType	No content type property is available in the AMQP message or when it is not “application/xml”.	
NoMessageID	The AMQP message does not contain the messageid.	
InvalidMessageType	The provided subject is null or unknown.	
NoReplyTo	The request AMQP message does not contain the reply-to.	
DigitalSignatureValidationFault	The Digital signature in not available or not valid.	

Table 40: Purple Profile Subscription Renew Response Message – SubscriptionRenewFault enumeration

The *UpdateSubscriptionFilterRequest* and *UpdateSubscriptionFilterResponse* messages are described in the tables below.

Element name	Type	Description	Note
Subscription Reference	SubscriptionReferenceType	The Subscription Reference provided as response message to subscription request.	
Message Content Selector	LengthRestrictedString	The filtering criteria replacing current Message Content Selector (if any).	Current Message Content Selector could be retrieved via the active subscriptions request message.

Table 41: Purple Profile UpdateSubscriptionFilter Request Message

In Table 42 the description of the UpdateSubscriptionFilterResponse message is provided. The message will include one and only one of the two elements (xsd:choice)

Element name	Type	Description	Note
Subscription	**SubscriptionType**	The descriptor of the updated subscription in case the request message is successfully processed.	SubscriptionType is described above.
Update Subscription Filter Processing Fault	**UpdateSubscriptionFilterFaultType**	Composite type containing the enumeration of faults associated with failure to process the request message and a string (free text) containing additional information about the fault.	The identified fault are described in the table below. The XSD has been designed for extensibility meaning that in addition to identified faults additional ones could be provided.

Table 42: Purple Profile UpdateSubscriptionFilter Response Message

Enumeration	Description	Note
UnknownSubscription Reference	The provided Subscription Reference is not known (no active subscription linked to that Subscription Reference)	
InvalidFilter	The request message contains a Filter that is evaluated as invalid.	
MalformedRequest	The request is not syntactically valid against the reference XML schema (payload) and properties.	
InfrastructureFault	An error occurred at infrastructure level.	

NoXMLContentType	No content type property is available in the AMQP message or when it is not "application/xml".	
NoMessageID	The AMQP message does not contain the messageid.	
InvalidMessageType	The provided subject is null or unknown.	
NoReplyTo	The request AMQP message does not contain the reply-to.	
DigitalSignatureValidationFault	The Digital signature in not available or not valid.	

Table 43: Purple Profile UpdateSubscriptionFilter Response Message – UpdateSubscriptionFilterFault enumeration

The *ActiveSubscriptionsNotify* message is described in the table below.

Element name	Type	Description	Note
Active Subscriptions	Collection of *SubscriptionType*	A collection of the active subscriptions of interest for the Air side subscription handler(s)..	

Table 44: Purple Profile ActiveSubscriptionsNotify Message

4.2.2.2.2 Messaging entities instantiation

AMQP 1.0 defines a wire level protocol for business messaging. The standard is suitable for all common business messaging behaviours and MEPs. The standard does not specify how to realize such MEPs but it provides a lower level peer-to-peer protocol on top of which is possible to build all common MEPs. In particular the standard does not mandate how to realize Publish/Subscribe MEPs or Request/Response MEPs. These considerations are applicable also to the entities and QoSs defined in the messaging characterization [Appendix B] and applicable to the Purple Profile (refer to functional view in §4.2.1 and statement of applicability in §B.2.1).

This specification aims at providing a technical layer enabling technical interoperability: building on top of the openness of AMQP 1.0 a concrete instantiation of Publish/Subscribe MEPs and Request/Response MEPs is designed and specified.

This section provides the instantiation over AMQP 1.0 of applicable entities defined in the messaging characterization (Table 45, Figure 37 and Figure 38) whereas QoSs mapping is provided in §4.2.2.2.3. Finally, additional AMQP specific considerations are provided in §4.2.2.5 where the interface bindings are defined.

Entity	AMQP 1.0 based instantiation
Message	AMQP 1.0 annotated message. The PP specification constrains which AMQP 1.0 annotated

Entity	AMQP 1.0 based instantiation
	message sections and fields have to be used and how (ref. §4.2.2.5).
Message Queue	The AMQP 1.0 core standard does not natively provide all the functionalities needed to instantiate this entity as defined in the characterization. This entity is instantiated as AMQP *distribution node* providing higher level PP specific messaging functionalities relying on AMQP 1.0 core standard. Higher level functionalities include messages store, routing, delivery and QoS related ones. Transport, messaging and security AMQP 1.0 functionalities are used to make the Message Queue reachable via AMQP 1.0 via addresses at link level (*source* or *target*) or at message level (*to* and *reply-to* AMQP standard fields). - Sender entity establishes an AMQP 1.0 link with the MQ entity with “source” link type (link type on the MQ side is “target”). - Receiver entity establishes an AMQP 1.0 link with the MQ entity with “target” link type (link type on the MQ side is “source”).
Sender	The AMQP 1.0 core standard refers to generic sending and receiving applications. In the MQ and MT characterization this entity has specific semantics in relationship with MQ entity. This entity is instantiated as AMQP node relying on AMQP 1.0 core standard to send messages to a MQ: - Sender entity establishes an AMQP 1.0 link with the MQ entity with “source” link type (link type on the MQ side is “target”). This entity in the context of the Purple Profile architecture could be: - PP specific messaging federation (routing). In this case higher level functionalities include message routing and annotated message use/processing as defined in this specification. - Application layer playing the requestor role (it sends request messages). In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification. - Application layer playing the responder role (it sends response messages). In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification.
Receiver	The AMQP 1.0 core standard refers to generic sending and receiving applications. In the MQ and MT characterization this entity has specific semantics in relationship with MQ entity. This entity is instantiated as AMQP node relying on AMQP 1.0 core standard to receive messages from a MQ: - Receiver entity establishes an AMQP 1.0 link with the MQ entity with “target” link type (link type on the MQ side is “source”). - PP specific messaging federation (routing). In this case higher level functionalities include message routing and annotated message use/processing as defined in this specification. - Application layer playing the requestor role (it receives response messages). In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification. - Application layer playing the responder role (it receives request messages). In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification.
Message Topic	The AMQP 1.0 core standard does not natively provide all the functionalities needed to instantiate this entity as defined in the characterization. This entity is instantiated as AMQP *distribution node* providing higher level PP specific messaging functionalities relying on AMQP 1.0 core standard. Higher level functionalities include messages store, routing, delivery and QoS related ones. Transport, messaging and security AMQP 1.0 functionalities are used to made the Message

Entity	AMQP 1.0 based instantiation
	Topic reachable over the network: - Publisher entity establishes an AMQP 1.0 link with the MT entity with “source” link type (link type on the MT side is “target”). - Subscriber entity establishes an AMQP 1.0 link with the MT entity with “target” link type (link type on the MT side is “source”). The interaction between this entity and the Subscription handler is not further specified because considered internal to the specific PP implementation (no impact on technical interoperability).
Publisher	The AMQP 1.0 core standard refers to generic sending and receiving applications. In the MQ and MT characterization this entity has specific semantics in relationship with MT entity. This entity is instantiated as AMQP node relying on AMQP 1.0 core standard to send messages to a MT: - Publisher entity establishes an AMQP 1.0 link with the MT entity with “source” link type (link type on the MT side is “target”). This entity in the context of the Purple Profile architecture could be: - PP specific messaging federation (routing). In this case higher level functionalities include message routing and annotated message use/processing as defined in this specification. - Application layer playing the publisher role. In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification.
Subscriber	The AMQP 1.0 core standard refers to generic sending and receiving applications. In the MQ and MT characterization this entity has specific semantics in relationship with MT entity. This entity is instantiated as AMQP node relying on AMQP 1.0 core standard to receive messages from a MT: - Subscriber entity establishes an AMQP 1.0 link with the MT entity with “target” link type (link type on the MT side is “source”). This entity interacts also with the Subscription handler. This interaction is realized via a pair of request and response MQs with subscriber and subscription handler entities behaving as sender and receive entities described above: - Subscriber entity creates and sends subscription/unsubscription/renew/retrieve active subscriptions request message. - Subscription handler entity processes subscription/unsubscription request messages. - Subscription handler entity creates and sends subscription/unsubscription response message. - Subscription handler entity maintains active subscriptions. - Subscriber entity processes subscription/unsubscription response messages. This entity in the context of the Purple Profile architecture could be: - PP specific messaging federation (routing). In this case higher level functionalities include message routing and annotated message use/processing as defined in this specification. - Application layer playing the subscriber role. In this case higher level functionalities include service specific functionalities and PP defined annotated message use as defined in this specification.
Subscription	The AMQP 1.0 core standard does not natively provide any functionalities concerning this entity. This entity is instantiated as PP defined message structures and logics (e.g. subscription status).
Subscription handler	The AMQP 1.0 core standard does not natively provide all the functionalities needed to

Entity	AMQP 1.0 based instantiation
	instantiate this entity as defined in the characterization. This entity is instantiated as AMQP node providing higher level PP specific messaging functionalities relying on AMQP 1.0 core standard. Higher level functionalities include subscriptions processing, subscription status handling and QoS related ones. Transport, messaging and security AMQP 1.0 functionalities are used to made the Subscription handler accessible over the network. The interaction with Subscriber entity is realized via a pair of request and response MQs with subscriber and subscription handler entities behaving as sender and receive entities described above: - Subscriber entity creates and sends subscription/unsubscription request message. - Subscription handler entity processes subscription/unsubscription request messages. - Subscription handler entity creates and sends subscription/unsubscription response message. - Subscription handler entity maintains active subscriptions. - Subscriber entity processes subscription/unsubscription response messages. The interaction between this entity and the MT is not further specified because considered internal to the specific PP implementation (no impact on technical interoperability).
Intermediary	Air and Ground Purple Profile SWIM Nodes providing PP defined messaging capabilities on top of AMQP 1.0. Air and Ground Purple Profile SWIM Nodes are *AMQP containers* as defined in the AMQP 1.0 core standard.

Table 45: Messaging entities instantiation over AMQP 1.0

Entities mapping in Table 45 has to be applied in accordance with PP technical architecture. In particular all the entities (MQs, Requestor, etc.) for Request/Response federated MEPs (§4.2.2.2.1.1) and those (MTs, Subscription handlers, etc.) for Publish/Subscribe federated MEPs (§4.2.2.2.1.2) have to be instantiated over AMQP 1.0 as described in this section.

MQ related mapping in Table 45 is depicted in Figure 37. The AMQP 1.0 core standard defined transactions functionalities are not depicted because not used in this specification. As described in Table 45, higher level functionalities provided by sender and receiver entities depend on the role played in the architecture. For simplicity the related functionalities are not depicted in Figure 37.

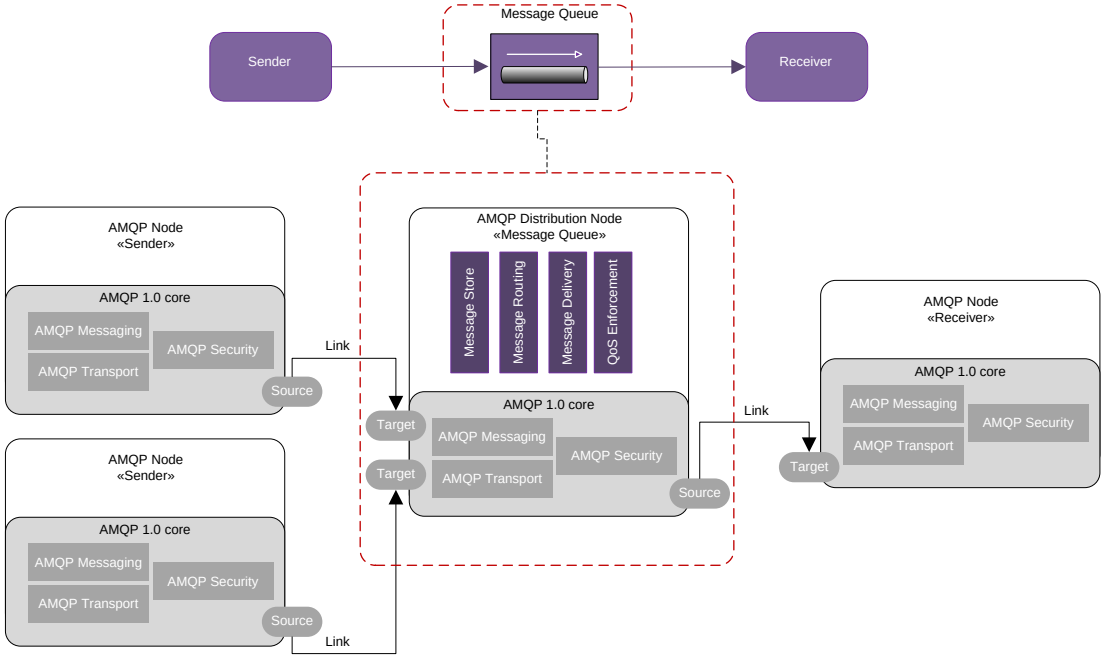


Figure 37: AMQP 1.0 based Message Queue(MQ)

MT related mapping in Table 45 is depicted in Figure 38. The AMQP 1.0 core standard defined transactions functionalities are not depicted because not used in this specification. As described in Table 45, higher level functionalities provided by publisher and subscriber entities depend on the role played in the architecture. For simplicity the related functionalities are not depicted in Figure 38.

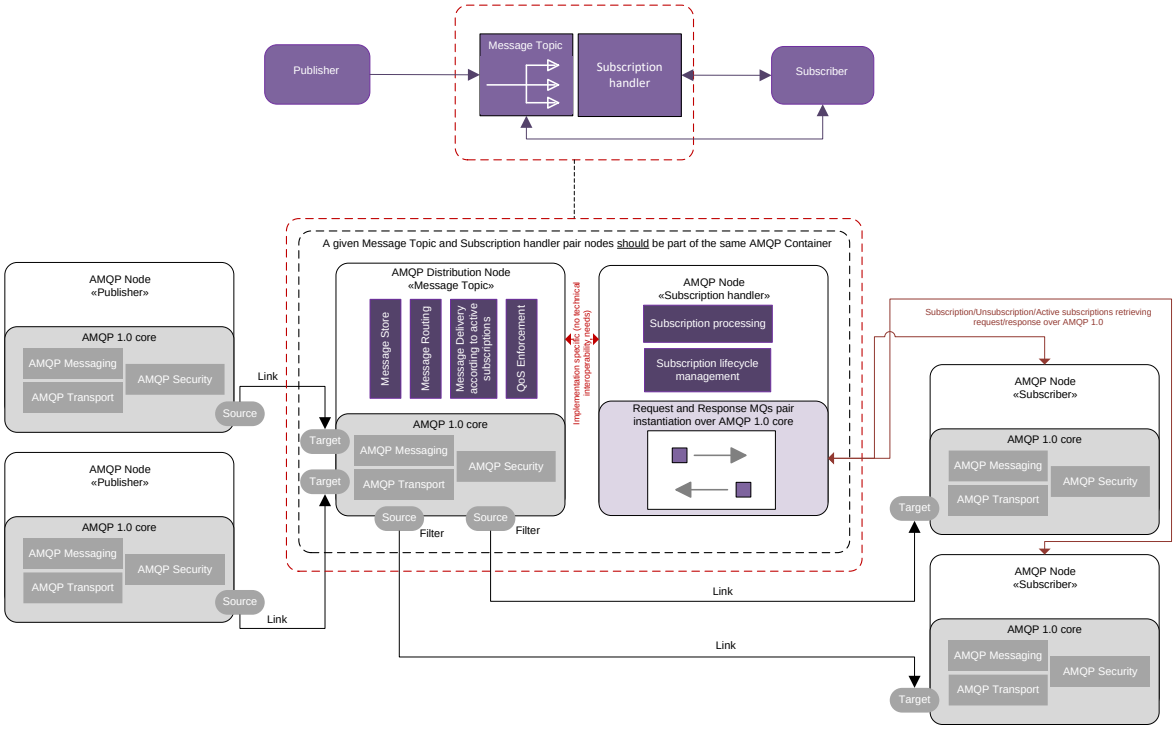


Figure 38: AMQP 1.0 based Message Topic(MT) and Subscription handler

In Figure 38 also the Subscription handler entity instantiation over AMQP 1.0 is depicted. It mainly consists in subscription management message flow described in §4.2.2.2.1.2 over request and response MQs. For simplicity of drawing the instantiation of this MQs pair over AMQP 1.0 is not depicted. Each of these subscription management queues are instantiated over AMQP as depicted in Figure 37:

- Subscriber entity behaving as Sender entity for subscription management request messages.
- Subscription handler entity behaving as receiver entity for subscription management request messages.
- Subscriber handler entity behaving as Sender entity for subscription management response messages.
- Subscriber entity behaving as receiver entity for subscription management response messages.

In accordance with messaging characterization [Appendix B] both MQ and MT entities are expected to provide synchronous and asynchronous message retrieving (in the case of MT this is related to the PSPUSH-MEP and PSPULL-MEP MEPs). The way these patterns are realized can be described at different levels. At AMQP link level these should be realized as follows:

- Synchronous message retrieving realized over AMQP 1.0 synchronous get (AMQP 1.0 core standard §2.6.8 [1]).

- Asynchronous message retrieving realized over AMQP 1.0 asynchronous notification (AMQP 1.0 core standard §2.6.9 [1]).

This specification is not constraining any API layer on top of AMQP.

4.2.2.2.3 Messaging Quality of service

This section describes how the messaging QoSs identified in the functional view (§4.2.1.1.1) are realized according to the technical architecture. Implementations of this mapping must comply with defined semantics and design constraints.

In addition to AMQP specificities, the QoSs instantiation is based on the messaging technical view and in particular to the MEPs described in §4.2.2.2.1.

4.2.2.2.3.1 Lifetime and durability

Table 46 provides the AMQP 1.0 based instantiation of applicable lifetime QoSs.

Entity	Lifespan/Lifetime QoS	AMQP 1.0 based instantiation
Message	Message with non-zero/specified lifespan	This QoS is instantiated as follows: - For all the messages the standard AMQP header *ttl* and AMQP Bare Message Standard properties *absolute-expiry-time* fields shall be provided. - Higher level PP functionalities to handle (filter & route) expired messages. Constraints: - Expired messages are filtered out and routed according to the applicable context-based routing policy. - Messages with undefined expiration time should be rejected or a default expiration time should be added.
Message Queue	Non-Temporary Queue	The AMQP 1.0 core standard does not natively provide all the functionalities needed to instantiate this QoS as defined in the characterization. Therefore, this QoS is recommended to be realized by higher level PP functionalities. However it should be evaluated the use of AMQP 1.0 Terminus Expiry Policy. In particular this QoS could be instantiated setting MQ *target* and *source* terminus *terminus-expiry-policy* to *never*. Constraints: - MQs lifecycle is management via administrative interfaces. - Temporary MQ are not allowed.
Message Topic	Non-Temporary Topic	The AMQP 1.0 core standard does not natively provide all the functionalities needed to instantiate this QoS as defined in the characterization. Therefore, this QoS is recommended to be realized by higher level PP functionalities. However it should be evaluated the use of AMQP 1.0 Terminus Expiry Policy. In particular this QoS could be instantiated setting MT *target* and *source* terminus *terminus-expiry-policy* to *never*. Constraints: - MTs lifecycle is management via administrative interfaces. - Temporary MT are not allowed.
Subscription	Subscription with zero/unspecified lifespan	The AMQP 1.0 core standard does not natively provide any functionality needed to instantiate this QoS as defined in the characterization. Therefore, this QoS is realized by

Entity	Lifespan/Lifetime QoS	AMQP 1.0 based instantiation
		higher level PP functionalities. Constraints: - Subscription management semantics and federation in accordance with this specification. - Subscription management messages in accordance with defined XSD. - Subscription management AMQP messages in accordance with this specification.
	Subscription with non-zero/specified lifespan	The AMQP 1.0 core standard does not natively provide any functionality needed to instantiate this QoS as defined in the characterization. Therefore, this QoS is realized by higher level PP functionalities. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts). - Subscription management semantics and federation in accordance with this specification. - Subscription management messages in accordance with defined XSD. - Subscription management AMQP messages in accordance with this specification.

Table 46: Purple Profile Lifespan/Lifetime QoS instantiation over AMQP 1.0

Table 47~~Table 47~~ provides the AMQP 1.0 based instantiation of applicable durability QoSs.

Entity	Durability QoS	AMQP 1.0 based instantiation
Message	Durable (recommended)	The standard AMQP header *durable* field shall be set to TRUE. In accordance with AMQP 1.0 core standard §3.2.1, this implies necessarily that the MQ/MT accepting durable messages are durable (see MQ and MT durability below).
	Non-Durable	The standard AMQP header *durable* field shall be set to FALSE. In this case it makes no sense to select the Durable Message Queue or Message Topic QoS. Volatile or non-durable MQ/MT should be used.
Message Queue	Non-Durable	This QoS is instantiated as follows: - The Non-Durable MQ over AMQP must reject messages with AMQP header *durable* field set to TRUE (AMQP 1.0 core standard §3.2.1). - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MQ AMQP Terminus durability to 0 (AMQP 1.0 core standard §3.5.5). This QoS makes sense only if a non-durable message QoS is required at message level. In order to guarantee this QoS end to end, all the MQs involved in the federation should be configured properly (in the more general case, they should be all non-durable).
	Volatile	This QoS is instantiated as follows: - The Volatile MQ over AMQP must reject messages with AMQP header *durable* field set to TRUE (AMQP 1.0 core standard §3.2.1). - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MQ AMQP Terminus durability to 1 (AMQP 1.0 core

Entity	Durability QoS	AMQP 1.0 based instantiation
		standard §3.5.5). This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). In order to guarantee this QoS end to end, all the MQs involved in the federation should be configured properly (in the more general case, they should be all volatile). The case where one or more of the MQs part of the federation have different durability (e.g. Non-durable, durable) is not considered in this specification and the expected end to end behaviour is not described.
	Durable (recommended)	This QoS is instantiated as follows: - The Durable MQ over AMQP must accept messages irrespective of AMQP header *durable* field value. - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MQ AMQP Terminus durability to 2 (AMQP 1.0 core standard §3.5.5). In order to guarantee this QoS end to end, all the MQs involved in the federation should be configured properly (in the more general case, they should be all durable).
Message Topic	Non-Durable	This QoS is instantiated as follows: - The Non-Durable MT over AMQP must reject messages with AMQP header *durable* field set to TRUE (AMQP 1.0 core standard §3.2.1). - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MT AMQP Terminus durability to 0 (AMQP 1.0 core standard §3.5.5). This QoS makes sense only if a non-durable message QoS is required at message level. In order to guarantee this QoS end to end, all the MTs involved in the federation should be configured properly (in the more general case, they should be all non-durable).
	Volatile	This QoS is instantiated as follows: - The Volatile MT over AMQP must reject messages with AMQP header *durable* field set to TRUE (AMQP 1.0 core standard §3.2.1). - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MT AMQP Terminus durability to 1 (AMQP 1.0 core standard §3.5.5). This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). In order to guarantee this QoS end to end, all the MQs/MTs involved in the federation should be configured properly (in the more general case, they should be all volatile). The case where one or more of the MTs/MQs part of the federation have different durability (e.g. Non-durable, durable) is not considered in this specification and the expected end to end behaviour is not described.
	Durable (recommended)	This QoS is instantiated as follows: - The Durable MT over AMQP must accept messages irrespective of AMQP header *durable* field value. - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the MT AMQP Terminus durability to 2 (AMQP 1.0 core standard §3.5.5). In order to guarantee this QoS end to end, all the MTs/MQs involved in the federation should be configured properly (in the more general case, they should be all durable).
Subscription	Non-Durable (Not applicable to aircraft subscriptions)	The AMQP 1.0 core standard does not provide any functionality related to this QoS. However. In accordance with semantics of this QoS defined in the characterization, no specific obligations for the MT are required. In order to save resources, the following is

Company General Use

Entity	Durability QoS	AMQP 1.0 based instantiation
		recommended: - MT AMQP Terminus expiry policy must be set to *link-detach* or *session-end* or *connection-close* (AMQP 1.0 core standard §3.5.6). Taking into account that Air PP SWIM Nodes are not always connected to the ground PP SWIM Nodes, this QoS is not allowed for aircraft subscriptions (aircraft subscribing to ground provided services).
	Durable (recommended)	The AMQP 1.0 core standard does not provide any functionality specific for this QoS. This QoS is instantiated as follows: - MT AMQP Terminus expiry policy set to *never* (AMQP 1.0 core standard §3.5.6). - Higher level messaging functionalities providing the semantics of this QoS as defined in the characterization. Taking into account that Air PP SWIM Nodes are not always connected to the ground PP SWIM Nodes, this QoS is the only allowed subscription QoS for aircraft subscriptions (aircraft subscribing to ground provided services). Ground applications subscribing to aircraft provided services may decide to use durable or non-durable subscriptions (assuming the service design will not constrain this QoS). However, this is the recommended Subscription durability QoS also for ground subscriptions.
Subscription handler	Volatile	This QoS is instantiated as follows: - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the Subscription handler AMQP Terminus durability to 1 (AMQP 1.0 core standard §3.5.5). This QoS does not guarantees that subscriptions are not lost irrespective of the subscription level durability QoS (durable or non-durable). In order to guarantee this QoS end to end, all the Subscription handlers involved in the federation should be configured properly (in the more general case, they should be all volatile).
	Durable (recommended)	This QoS is instantiated as follows: - It should be evaluated the use of AMQP 1.0 Terminus durability. In particular this QoS could be instantiated setting the Subscription handler AMQP Terminus durability to 2 (AMQP 1.0 core standard §3.5.5). - Higher level messaging functionalities providing the semantics of this QoS as defined in the characterization. In order to guarantee this QoS end to end, all the Subscription handlers involved in the federation should be configured properly (in the more general case, they should be all durable). The case where one or more of Subscription handlers have different durability (e.g. volatile) is not considered in this specification and the expected end to end behaviour is not described. This is the recommended Subscription handler durability QoS. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts).

Table 47: Purple Profile durability QoS instantiation over AMQP 1.0

4.2.2.2.3.2 Delivery guarantees

Table 48 provides the AMQP 1.0 based instantiation of delivery guarantees QoSs. For some delivery guarantees some constraints are provided. In particular, for At-Least-Once and Exactly-Once delivery

guarantees it is important to take into account constraints on the message, MQ, MT and subscription handler durability.

Delivery guarantees	Delivery guarantee	AMQP 1.0 based instantiation
Point-to-point	At-Most-Once	Point-to-point delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality over AMQP 1.0 standard settling and link resume transport level mechanisms (AMQP 1.0 core standard §2.6.12). Link recovery is not initiated by MQ, MT and Subscription handler. It is up to sender, receiver, publisher and subscriber entities to initiate link recovery. At-Most-Once point-to-point delivery guarantees is instantiated as follows: - sending entity (Sender, Publisher) must settle the delivery before sending the message. - higher level messaging functionalities to configure and to enforce the settling strategy/policy.
	At-Least-Once (recommended)	Point-to-point delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality over AMQP 1.0 standard settling and link resume transport level mechanisms (AMQP 1.0 core standard §2.6.12). Link recovery is not initiated by MQ, MT and Subscription handler. It is up to sender, receiver, publisher and subscriber entities to initiate link recovery. At-Least-Once point-to-point delivery guarantees is instantiated as follows: - sending entity (Sender, Publisher) must not settle the delivery before sending the message. - receiving entity (MQ, MT, Receiver, Subscriber) must settle the delivery immediately upon processing the message. - higher level messaging functionalities to configure and to enforce the settling strategy/policy. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts). - Message durability must be durable. - MQ, MT and Subscription handler durability must be durable.
	Exactly-Once	Point-to-point delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality over AMQP 1.0 standard settling and link resume transport level mechanisms (AMQP 1.0 core standard §2.6.12). Link recovery is not initiated by MQ, MT and Subscription handler. It is up to sender, receiver, publisher and subscriber entities to initiate link recovery. Exactly-Once point-to-point delivery guarantees is instantiated as follows: - sending entity (Sender, Publisher) must settle the delivery when the receiver reaches a terminal state. - receiving entity (MQ, MT, Receiver, Subscriber) must settle the delivery when the sending entity settles. - higher level messaging functionalities to configure and to enforce the settling strategy/policy. Alternatively, the above could be replaced/complemented by At-Least-Once semantics enriched with: - higher level messaging functionalities receiving entity side to detect and filter-out duplicated messages (PP uses UUID for message-id). Constraints:

Delivery guarantees	Delivery guarantee	AMQP 1.0 based instantiation
		- Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts). - Message durability must be durable. - MQ, MT and Subscription handler durability must be durable.
	No delivery guarantees (Not allowed for air-ground connections)	None of the obligations described for At-Most-Once, At-Least-Once and Exactly-Once point-to-point delivery guarantees QoSs is applicable. Constraints: - This QoS is not allowed for air-ground connections (Air SWIM Node connects to Ground SWIM Node MQ/MT (internal to the TI connections and bindings).
End-to-end	At-Most-Once	AMQP 1.0 core standard is a peer-to-peer protocol and it does not provide any specific end-to-end delivery guarantees functionality. End to end delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality composed with point-to-point delivery guarantees and durability QoSs. MQ At-Most-Once delivery guarantees is instantiated as follows: - At-Most-Once point-to-point delivery guarantees shall be set for both Sender-MQ and MQ-Receiver connections. - Taking into account that this end to end QoS does not guarantee that messages are not lost there are no obligations for the MQ durability QoS. However, in order to save messaging resources, MQ durability QoS should be set to Non-durable or Volatile. MT At-Most-Once delivery guarantees is instantiated as follows: - At-Most-Once point-to-point delivery guarantees shall be set for both Publisher-MT and MT-Subscriber connections. - Taking into account that this end to end QoS does not guarantee that messages are not lost there are no obligations for the MT durability QoS. However, in order to save messaging resources, MT durability QoS should be set to Non-durable or Volatile.
	At-Least-Once (recommended)	AMQP 1.0 core standard is a peer-to-peer protocol and it does not provide any specific end-to-end delivery guarantees functionality. End to end delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality composed with point-to-point delivery guarantees and durability QoSs. MQ At-Least-Once delivery guarantees is instantiated as follows: - At-Least-Once point-to-point delivery guarantees shall be set for both Sender-MQ and MQ-Receiver connections. - MQ durability QoS must be set to Durable. MT At-Least-Once delivery guarantees is instantiated as follows: - At-Least-Once point-to-point delivery guarantees shall be set for both Publisher-MT and MT-Subscriber connections. - MT durability QoS must be set to Durable. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts).
	Exactly-Once	AMQP 1.0 core standard is a peer-to-peer protocol and it does not provide any specific end-to-end delivery guarantees functionality. End to end delivery guarantees QoSs defined in the characterization are realized by higher level messaging functionality composed with point-to-point delivery guarantees and durability QoSs. MQ Exactly-Once delivery guarantees is instantiated as follows: - Exactly-Once point-to-point delivery guarantees shall be set for both Sender-MQ and MQ-Receiver connections. - MQ durability QoS must be set to Durable.

Delivery guarantees	Delivery guarantee	AMQP 1.0 based instantiation
		MT Exactly-Once delivery guarantees is instantiated as follows: - Exactly-Once point-to-point delivery guarantees shall be set for both Publisher-MT and MT-Subscriber connections. - MT durability QoS must be set to Durable. Additional Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts).
	No delivery guarantees	None of the obligations described for At-Most-Once and At-Least-Once end to end delivery guarantees QoSs is applicable.

Table 48: Purple Profile Delivery guarantees QoS instantiation over AMQP 1.0

In the messaging characterization [Appendix B] some non-nominal cases have been identified and analysed in relationship with delivery guarantees. Table 49 provides the results of this analysis.

Event	Delivery guarantee	Analysis
Connection establishment failure	At-Most-Once or No delivery guarantees	Message not delivered event due to Connection establishment failure event is acceptable. In this case it is not strictly needed that the reconnection event will follow.
	At-Least-Once or Exactly-Once delivery guarantees	Message not delivered event due to Connection establishment failure event is not acceptable. In this case the reconnection event will follow. This is necessary but not sufficient condition for these guarantees. In particular also reconnection event(s) may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc. Depending on the criticality, events like "*Message not delivered event due to Reconnection establishment failure when At-Least-Once delivery guarantee is required*" should be logged and traced. Furthermore, the event should be also reported (e.g. monitoring capabilities).
Abnormal disconnection	At-Most-Once or No delivery guarantees	Message not delivered event due to Abnormal disconnection event is acceptable. In this case it is not strictly needed that the reconnection event will follow.
	At-Least-Once or Exactly-Once delivery guarantees	Message not delivered event due to Abnormal disconnection event is not acceptable. In this case the reconnection event will follow. This is necessary but not sufficient condition for these guarantees. In particular also reconnection event(s) may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc. Depending on the criticality, events like "*Message not delivered event due to abnormal disconnection when At-Least-Once delivery guarantee is required*" should be logged and traced. Furthermore, the event should be also reported (e.g. monitoring capabilities).
Reconnection establishment failure	At-Most-Once or No delivery guarantees	Message not delivered event due to Reconnection establishment failure event is acceptable. In this case it is not strictly needed that additional reconnection event(s) will follow. (e.g. different addresses and/or retries).
	At-Least-Once or Exactly-Once delivery guarantees	Message not delivered event due to Reconnection establishment failure event is not acceptable. In this case additional reconnection event(s) will follow. (e.g. different addresses and/or retries). This is necessary but not sufficient condition for these guarantees. In particular also these events may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc. Depending on the criticality, events like "*Message not delivered event due to reconnection establishment failure when At-Least-Once delivery guarantee is required*"

Event	Delivery guarantee	Analysis
		should be logged and traced. Furthermore, the event should be also reported (e.g. monitoring capabilities).
Message not delivered	At-Most-Once or No delivery guarantees	Message not delivered event is acceptable. Logging of this event is not mandatory.
	At-Least-Once or Exactly-Once delivery guarantees	Message not delivered event is not acceptable. This represents an anomaly to be properly logged, traced and reported.
Message dropped	At-Most-Once or No delivery guarantees	Message dropped event is acceptable. Logging of this event is not mandatory
	At-Least-Once or Exactly-Once delivery guarantees	Message dropped event is not acceptable. This represents an anomaly to be properly logged, traced and reported.

Table 49: Non-nominal events and delivery guarantees

For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are initiated by the peer initiating the connection/reconnection. Irrespective of the cardinalities, taking into account the technical architecture, the 3 types of required connections are depicted in Figure 39:

- (Purple Profile enabled SWIM service delivery guarantees) A connection is established towards the Air SWIM Node in order to allow aircraft applications to send/publish or receive messages. This is the connection used to create the session and the link concerning “Service bindings”. This interfacing layer has to behave according to the chosen delivery guarantees for that specific Purple Profile enabled SWIM service.
- The Air SWIM Node establishes connection(s) towards Ground SWIM Node(s) in order to be able to federate the MEPs. This is the connection used to create the session and the link concerning “Internal service bindings”. Depending of MQs segregation (used for more than one services, etc.) this interfacing layer has to behave according to the chosen delivery guarantees for the specific/group of Purple Profile enabled SWIM service/s.
- (A/C consuming ground services) The Ground SWIM Node establishes connection(s) towards ground AMQP containers hosting ground services resources. This is the connection used to create the session and the link concerning “Service bindings”. This interfacing layer has to behave according to the chosen delivery guarantees for that specific Purple Profile enabled SWIM service.
- (Ground consuming aircraft provided services) Ground application establishes connection(s) towards Ground SWIM Node in order to be able to consume aircraft provided services. This is the connection used to create the session and the link concerning “Service bindings”. This interfacing layer has to behave according to the chosen delivery guarantees for that specific Purple Profile enabled SWIM service.

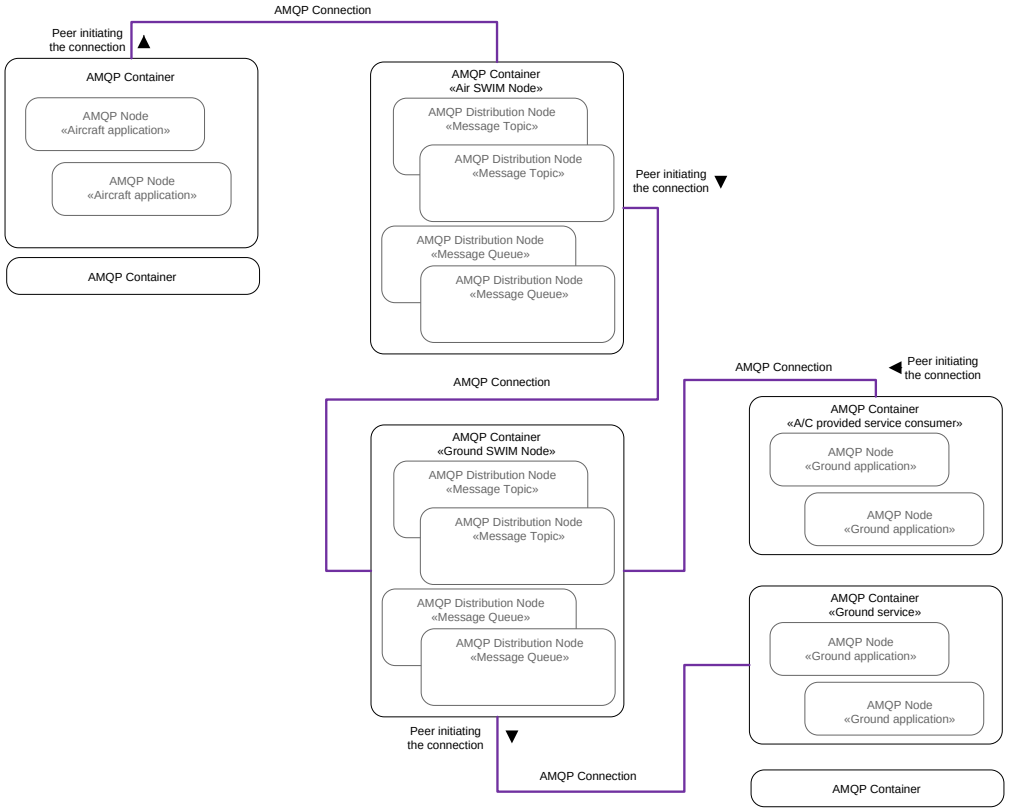


Figure 39: AMQP Connections and entities initiating the connection

Summarizing reconnection and retry policies concern:

- Application layer: Purple Profile aircraft and ground applications.
- SWIM-TI layer:
  - Air SWIM Node connecting to Ground SWIM Node(s).
  - Ground SWIM Node connecting to ground SWIM service(s).

Table 50 provides the minimum set of information/parameters configurable via the reconnection and retry policy. These parameters are widely supported out of the box by most AMQP-compliant messaging products. It is expected that such logics should be configurable per-SWIM service, per-SWIM service class or per SWIM Node.

Parameter	Definition
Max reconnection attempts	The maximum number of reconnection attempts allowed before reporting the failure. Constraints: - default value for disabling the reconnection has to be supported. - it should not be possible to retry forever.
Initial Reconnection/Retry	The amount of time the connecting peer waits before the first attempt to reconnect to a remote peer.

Parameter	Definition
delay	
Reconnection/retry delay	The amount of time between successive reconnection attempts.
Exponential back-off	This allows to apply the exponential back-off algorithm in the successive reconnection attempts. Following sub-parameters could be configurable: - enable/disable the use of the exponential back-off algorithm. When disable the reconnection delay between successive reconnection attempts remains constant (*Reconnection/retry delay* parameter above) - the multiplier for growing successive reconnection attempts according to the algorithm. - maximum reconnection delay to limit the maximum delay evaluated by the algorithm.
Connection URIs	One or more URIs to connect to in case of connection/reconnect failure. These URIs could be logical names and physical addresses (IP + port). In case a single URI is provided the reconnection attempts will use the same URI. This could be a logical name mapped to one or more physical addresses. This specification is not defining how the two or more replicas should be synchronized. An open and standard (AMQP) based approach is recommended. When more than one URI is provided, the policy has to allow to configure the order used to try the available URIs: - list based order, - randomly. The available URIs could be updated: - the policy should allow to update it at run-time without restarting software system/sub-system. - there are AMQP 1.0 core, legacy and draft AMQP based standards/mechanism (e.g. AMQP 1.0 core “amqp:connection:redirect” error, draft OASIS “Connection Failover Properties”) allowing the “connection” server to provide the client with available alternate URIs. These solutions are not mandated by this specification.

Table 50: Reconnection and retry policy

A variety of anomalies can cause a hang status in one of the connecting peer. In some cases such hangs cannot be undone by the action of a single peer and may exclusively block resources at the side of the other peer (e.g. connection closed by server peer but in the TCP TIME_WAIT state). Connection-oriented messaging protocols may support time out mechanisms on top of timeout mechanisms already present in underlying transport protocols such as TCP. In such case time-out mechanisms at the level of the messaging protocol are useful to detect in a timely manner an anomaly that could be hidden for a long time by an underlying complex of transport and network protocols.

Two mechanisms with low overhead complement each other in the ability to detect such cases and to free exclusively blocked resources: the idle-time-out in the AMQP 1.0 core open performative (aka “heartbeat”) and the “Keep Alive” mechanism at TCP level. As the “Keep Alive” mechanism at TCP level may not yield the desired and/or expected effect it is necessary to be able to switch it off.

Furthermore, a number of behaviours at TCP level are derived from the Maximum Segment Lifetime (MSL) for TCP (RFC 793, default value is 2 minutes) including intentionally keeping quiet for a while (TCP Quiet Time concept, MSL duration), as well as the timeout on TIME_WAIT state, which is set by default at 2 * MSL (i.e. 4 minutes by default), as well the upper bound for RTO (Retransmission Timeout as in RFC 793) (2 * MSL, i.e. 4 minutes by default).

While it is expecting that the software environment will allow to properly configure (when needed) different values for MSL (2 minutes or less) and RTO (significantly below the default upper bound of 4 minutes), it makes sense to identify lower and upper bounds for the AMQP idle-time-out:

- Too short idle-time-out could lead to excessive load and unnecessary clean-up needing retries.
- Too long idle-time-out could lead to too long blocking of resources in case of anomaly.

The upper bound could be evaluated starting from default MSL and RTO: an AMQP idle-time-out of 5 minutes (2 * MSL + 1 minute or 300000 milliseconds) provides sufficient time to lower protocol layers to clean up, recover and/or get back into a known and controlled state. If after 5 minutes this is not case, then the AMQP 1.0 idle-time-out will kick in and may help to detect and recover from such states.

The lower bound could be evaluated taking into account lifetime of messages: a lower bound shorter than the message expiration time introduces generate unnecessary traffic. Advisory SWIM services concern aeronautical and weather data with different lifetime. Taking into account that it is not possible to have an exhaustive analysis of all the candidate Purple Profile enabled SWIM services, a lower bound of 1 minute (60000 milliseconds) is considered.

The AMQP idle-time-out shall be configurable per AMQP connections and it shall not be less than 60000 milliseconds and shall not be higher than 300000 milliseconds.

4.2.2.2.3.3 Ordering guarantees

Table 51 provides the AMQP 1.0 based instantiation of applicable ordering guarantees QoSs.

Entity	Ordering guarantees QoS	AMQP 1.0 based instantiation
Message	Message priority	The standard AMQP header *priority* field shall be used to specify the message priority. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts). - Message Priority based ordering for Message Queue or Message Topic is required. It makes no sense to use message priority with FIFO ordering for Message Queue or Message Topic.
	Message with default priority	Any value shall be provided in the standard AMQP header *priority* field. The default priority is assigned to that message. Constraints: - FIFO ordering for Message Queue or Message Topic is required. It makes no sense to use message priority based ordering for Message Queue or Message Topic.
Message Queue	FIFO	This QoS is instantiated as follows: - Any value shall be provided in the standard AMQP header *priority* field. The default priority is assigned to that message. - Higher level PP functionalities (store, routing and delivery) to ensure end to end FIFO ordering between senders and receiver. This is applicable for all the MQs in the routing path.
	Message Priority (best effort)	This QoS is instantiated as follows: - The standard AMQP header *priority* field shall be used to specify the message priority. - Higher level PP functionalities (store, routing and delivery) to ensure end to end

Company General Use

Entity	Ordering guarantees QoS	AMQP 1.0 based instantiation
		message priority based ordering between senders and receiver. This is applicable for all the MQs in the routing path. How this is designed and implemented is internal to SWIM Node implementation. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts).
Message Topic	FIFO	This QoS is instantiated as follows: - Any value shall be provided in the standard AMQP header *priority* field. The default priority is assigned to that message. - Higher level PP functionalities (store, routing and delivery) to ensure end to end FIFO ordering between senders and receiver. This is applicable for all the MQs/MTs in the routing path.
	Message Priority (best effort)	This QoS is instantiated as follows: - The standard AMQP header *priority* field shall be used to specify the message priority. - Higher level PP functionalities (store, routing and delivery) to ensure end to end message priority based ordering between publishers and subscribers. This is applicable for all the MQs in the routing path. How this is designed and implemented is internal to SWIM Node implementation. Constraints: - Optional Profile part (<PP Ground Advanced> and <PP Air Advanced> profile parts).

Table 51: Purple Profile Ordering guarantees QoS instantiation over AMQP 1.0

4.2.2.2.3.4 On-the-fly compression

Data compression can be realised in more than one way and at distinct levels. The ATM application layer can provide a compressed payload to the SWIM-TI. In this case (perimeter between ATM and SWIM-TI layers) the TI is only responsible for routing the message to the intended recipients.

The SWIM-TI itself can also provide data compression (on-the-fly compression). This is an advanced capability that could be useful when application level messages are not optimized in terms (e.g.) of message size for the uplink. Examples could be uplink of AIXM or WXXM data from the ground in a many to many information exchange: irrespective of A/C specific filtering criteria such data could be published and available for aircraft and ground applications: the publisher is not implementing subscribers specific data representation. In this case, the messages between Air and Ground SWIM Node could be compressed on-the-fly in a way transparent to the publisher and subscriber: the publisher publishes uncompressed message and the aircraft subscriber receives an uncompressed message. The TI is handling the payload as a sequence of bytes compressing and uncompressing it when needed (threshold based compression is supported).

When compression is composed with encryption cryptography techniques the following is recommended:

- Compression at application level: it is recommended to first compress and then to encrypt. This provides a more efficient compression.
- Compression internal to SWIM-TI: not applicable because inefficient compression rate.

For both application layer and on-the-fly compression only the following compression standards are allowed (to be interpreted as per section 3.5 of RFC 2616):

- GZIP (RFC 1952) compressed original MIME type (e.g. GZIP compressed XML METAR).
- Deflate (RFC 1951) compressed original MIME type (e.g. deflate compressed XML METAR) inside the zlib data format (RFC 1950).

For application layer compression the AMQP Bare Message Standard properties content-type and content-encoding fields have to be used as in Table 52.

AMQP Bare Message Standard property	Restricted use
content-type	The RFC-2046 MIME type for the message payload.
content-encoding	As per section 3.5 of RFC 2616. It is used to provide compression standards used to compress original media type. Used in combination with content type property. Allowed encoding (refer to HTTP Content Coding Registry) are: - "gzip": GZIP (RFC 1952) compressed original MIME type. - "deflate": Deflate (RFC 1951) compressed original MIME type inside the zlib data format (RFC 1950).

Table 52: AMQP content-type and content-encoding for application level compression

For on-the-fly compression, a PP defined AMQP message annotation is used (Table 53). This annotation is added by the distribution node compressing on the fly the data. On receiving a message with this annotation, the MQ/MT AMQP node to which the final application level recipient is connected to, is responsible for uncompressing the data.

AMQP message annotation	Value	Description
key	x-ontheflycompressed	This indicates that the payload (Bare Message Application Data) has been compressed on the fly by a distribution node. In accordance with AMQP 1.0 core, on receiving this annotation key, if not supported the receiving AMQP container MUST detach the link with a not-implemented error. However this should never occur because all the messaging resources and capabilities are agreed and configured in advance.
value	gzip|deflate	This indicates the compression algorithm used.

Table 53: AMQP message annotation for on-the-fly compression

Finally, on-the-fly compression is an advanced allocated to an optional Profile parts ((<PP Air Advanced> and <PP Ground Advanced>).

4.2.2.3 Security

In this section the Purple Profile security technical view is described. It aims at describing the "how" and "how good" concerning the security functions introduced in the functional view (§4.2.1) taking into account functional view's requirements (§4.3.1), security risk assessment (§4.2.1.1.2), messaging technical view (§4.2.2.2), applicable constraints (e.g. §4.2.2.1.6), and design decisions.

End-to-end security needs introduced in §4.2.1.1.2 and §4.2.1.1.3 became apparent when assessing the messaging technical view: the end to end message distribution is realized via multiple AMQP distribution nodes (at least two) and connections (e.g. refer to Figure 39).

The Purple Profile is in charge of ensuring point-to-point security via transport level security mechanisms. This is further detailed below in §4.2.2.3.2.

The Purple Profile is not responsible for end-to-end security: this is delegated to the Purple Profile enabled applications. The Purple Profile aims at enabling the transfer of security information (when needed) without violating message's security attributes. This is further detailed below in §4.2.2.3.3.

It is anticipated that transport and message level security mechanisms could be eventually properly combined with network level security (e.g. IPSec tunnelling). Although the presence of such security controls is transparent for the Purple Profile it has to be said that transport level security has been designed assuming unsecure network (e.g. no IPSec tunnelling).

Technical view security requirements are provided in §4.3.5 and §4.3.7 (bindings level).

4.2.2.3.1 Identity Management

Purple Profile security technical view is based on the adoption of constrained set of cryptographic keys and algorithms and on the X.509 version 3 certificates as digital identity type.

X.509v3 certificates and cryptographic keys are managed via Public Key Infrastructure (PKI) that encompasses administrative procedures and local and remote resources and services. Furthermore, in the Aviation domain a number of regulations and standards exist to properly manage Aviation cybersecurity.

The Purple Profile is not responsible for defining and/or identifying applicable regulations and procedures: without being exhaustive and complete, applicable regulations and standards have been considered and referred by requirements.

Public Key Infrastructure (PKI) consists of a set of standards, procedures, software, and people for implementing authentication/authenticity, authorization, confidentiality and integrity using public key cryptography. In particular the PKI provides the means for requesting, installing, configuring, validating, managing and revoking X.509 certificates used for digital signature, encryption, authentication and authorization (Attribute Based Access Control supported by X.509 certificate attributes).

Within the PKI the Certification Authority (CA) is responsible for creating, signing, emitting and maintaining X.509 certificates and revocation lists (CRL). In particular the CA covers three main functions:

- The Certificate Management that issues certificates and maintains certificates revocation lists.
- The Registration Authority (RA) is the administrative function in charge of registration of entities in the Public Key Infrastructure (PKI).

- The Validation Authority (VA) is the function in charge of validation of the certificates.

In this section, the technical view refers in general to CA irrespective of possible deployment options such as the Bridge CA and CA delegation (or hierarchical PKI). At technical level, the CA provides capabilities used by the Purple Profile enabled applications and SWIM Nodes irrespective of how the trust-relationship between subordinate CAs and/or root CAs is established. The reference for the identified bindings is the SESAR 1 SWIM Identity Management Technical Specification [53].

Authentication based on X.509v3 certificates encompasses following main steps:

- The X.509v3 certificate is not expired: this step is enforced comparing the expiration date and time of the certificate against current date and time. This does not rely on local/remove resources or services and it requires clock synchronization with proper accuracy.
- The X.509v3 certificate has been issued by a trusted CA: this step could be enforced via both local and/or remote services. The Purple Profile requires that a trust exists with the issuing CA: the simpler way to achieve that is to add the CA's X.509v3 certificate in the trust-store (resource available locally to the entity validating the certificate).
- The X.509v3 certificate has not been revoked: this step is enforced by:
    - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or
    - Consuming OCSP (Online Certificate Status Protocol) service(s), or
    - Combining both CRL and OCSP based certification revocation status mechanisms.

In the Purple Profile the basic (<PP Core>) option for checking X.509 certificate revocation status is to rely on locally stored CRLs. The capability of Purple Profile enabled applications and SWIM Nodes to use OCSP based revocation status check is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts).

In §4.2.2.3.4 a sub-set of non-nominal security cases concerning X.509 certificate validation are described.

CRLs are periodically issued by the CAs and typically installed/updated locally as part of maintenance activities. Three additional aspects concerning the CRLs have been evaluated:

- The CRLs expire: an expired CRL represents a possible vulnerability. When it is not possible to update on-the-fly the expired CRL, the revocation status check will fail. A standard mechanism allowing the retrieving of CRLs is the CRL distribution point (CDP). CAs typically provide online CDPs over HTTP (HTTP CDP) and/or over LDAP (LDAP CDP) and the endpoint addresses of these services could be also included in the certificates they issue.

  Basic (<PP Core>) Purple Profile option is based on a scheduled maintenance process ensuring that CRL are updated before they expire.

  The capability of Purple Profile enabled applications and SWIM Nodes to use HTTP CDPs and/or LDAP CDPs is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts).
- Delta-CRL: this mechanism allows relying party to download (via CDPs) the large CRL (base CRL) less frequently and the Delta more frequently. Advanced Purple Profile enabled applications and SWIM Nodes conformant to <PP Air Security+> and <PP Ground Security+> profile parts have to be able to handle delta-CRLs.

- CRL partitioning: this an additional mechanism typically provided by CAs to cover some cases including (but not limited to) large CRLs. Advanced Purple Profile enabled applications and SWIM Nodes conformant to <PP Air Security+> and <PP Ground Security+> profile parts have to be able to handle CRL partitioning.

Typically for all the security infrastructure based on PKI, at infrastructure level there are protected stores used to store X.509 certificates, keys, CRLs and trusted certificates. These stores could be at infrastructure layer or not: concerning enterprise are not forced to create SWIM specific stores and when the capability is available it is recommended to reuse it. This is especially relevant for the aircraft where potentially several entities need to access and to check X.509v3 related information.

A possible option providing concerned aircraft components with a consistent access to these information (e.g. avoid duplication of stores/CRLs) could be to have a local (i.e. on-board) trusted OCSP responder: aircraft applications and Air SWIM Node use this local OCSP responder to check the status of certificates. The OCSP relies on local store(s) subject to maintenance and updates (e.g. CDPs). This is only an illustrative example: the Purple Profile is not responsible for the complete aircraft architecture and it is not mandating any specific deployment option.

4.2.2.3.2 Point to point (transport level) security

As anticipated above, the Purple Profile is in charge of ensuring point-to-point security via transport level security mechanisms while providing mechanisms to distribute message level security information.

Transport level security applies to all the directly connected messaging entities in the messaging technical view described in §4.2.2.2.1: access to message queues, message topics and subscription handlers is mutual authenticated, authorized and protected in terms of confidentiality and integrity.

The adopted transport level security mechanism is IANA *amqps* as defined in the AMQP 1.0 §5.2.1 with following TLS level constraints:

- Fallback from TLS 1.3 to TLS 1.2 is allowed.
- Fallback to any TLS or SSL version lower than TLS 1.2 is prohibited.

In Table 54 the traceability between the “what” and the “how” is provided.

Function	“What” to “How”
Authentication	Mutual transport level authentication of AMQP 1.0 peers through TLS 1.2 or TLS 1.3 according to the *amqps* form only.
Authorization	The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers).
Audit	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.
Confidentiality ensuring	Transport level confidentiality is provided through TLS 1.2/1.3 standard mechanisms.
Information Integrity and authenticity ensuring	Transport level integrity and authenticity are provided through TLS 1.2/1.3 standard mechanisms.

Message screening	No technical interoperability needs have been recognized. The Purple Profile is not constraining the "how". The functional view requirements concerning this function represent the reference for prototyping activities.
Overload protection	No technical interoperability needs have been recognized. The Purple Profile is not constraining the "how". The functional view requirements concerning this function represent the reference for prototyping activities.
Security Policy management	No technical interoperability needs have been recognized. The Purple Profile is not constraining the "how". The functional view requirements concerning this function represent the reference for prototyping activities.

Table 54: Security functional view to technical view

4.2.2.3.3 End to end (message level) security

The AMQP 1.0 core specification does not constrain the options to add message level security. There are many existing open standards for signing and/or encryption of messages that could be used inside a message payload.

The Purple Profile provides two mechanisms to transfer message level security information from the sender to the intended recipient(s):

- Security information attached to the data: the application-data section within the AMQP bare message includes both data and security information (e.g. digital signature). Examples of applicable standards are S/MIME 3.2 [54], XML signature [56] and XML encryption [55].
- Security information detached from the data: the application-data section within the AMQP bare message includes plain or encrypted data and cryptographic information (message digest, digital signature, etc.) are included in the AMQP 1.0 footer section. The AMQP 1.0 core standard requires that a *registry of defined footers and their meanings is maintained* but at the time of writing this specification (January 2019) no footers have been registered.

Both mechanisms could be characterized with pros and cons: the Purple Profile supports both and it is up to Purple Profile enabled SWIM service architects to use one of none of these mechanisms. Furthermore, future SWIM standardization activities could provide more constraints in favour of one or the other option.

In Table 55 below, Purple Profile specific constraints for both mechanisms are provided.

Message level security mechanism	Applicable standards	AMQP annotated message section(s)	Restricted use
Security information attached to the data	XML Encryption, XML Signature	**content-type** AMQP Bare Message Standard property	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service design (e.g. application/xml for XML). It should be noticed that XML Encryption and XML Signature could be used also for non-XML data.
	S/MIME 3.2 (RFC 5751)	**content-type** AMQP Bare Message Standard property	It shall be set to the outer MIME type of the S/MIME message and only media types included in the S/MIME 3.2 chapter 3.9 are

Message level security mechanism	Applicable standards	AMQP annotated message section(s)	Restricted use
			allowed.
		AMQP Bare message application-data section	The entire S/MIME message including all levels of nesting and wrapping shall be provided in a single AMQP Bare message application-data section. Constraints for backward compatibility with prior versions of S/MIME and constraints related to 7-bit transfer encoding are not applicable. Furthermore, as there are different ways to use S/MIME 3.2, further details have to be documented as part of the SWIM service design specification.
	Any additional standard	AMQP Bare message	The use of the standard and additional restricted use of any AMQP Bare message sections shall be documented as part of the SWIM service design specification.
Security information detached from the data	HMAC (RFC 2104)	**content-type** AMQP Bare Message Standard property	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service design.
		footer section , key=**HMAC**	value= semicolon separated ***HMAC-Algorithm***, ***HMAC-Target, HMAC-Digest*** *and* ***HMAC-Secret***. HMAC-Algorithm: HMAC cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. In all the cases, the selected algorithm must comply with applicable security policies, best practices and regulations. HMAC-Target: {bare, data}. It indicates if the HMAC is calculated on the entire AMQP bare message ("bare") or only on the application-data section ("data"). HMAC-Digest: Base64 encoded message digest. HMAC-Secret: optional field containing one or more comma separated "uuid" and "secret" pairs. For each intended recipient a colon separated "uuid" and "secret" pair is provided. The uuid is the name-based UUID of the recipient and the "secret" is the symmetric key encrypted with the recipient's public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The "uuid" and "secret" pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e. publication messages) a mechanism should be put in place in order to

Message level security mechanism	Applicable standards	AMQP annotated message section(s)	Restricted use
			allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid" and "secret" pairs in accordance with active subscribers' UUIDs. Taking into account the potential number of recipients, the full set of "uuid" and "secret" pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.
	Digital Signature	**content-type** AMQP Bare Message Standard property	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service design.
		footer section , key=**DSGN**	value= semicolon separated ***DSGN-Algorithm***, ***DSGN-Target*** and ***DSGN-Signature***. DSGN-Algorithm: Digital signature cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. In all the cases, the selected algorithm must comply with applicable security policies, best practices and regulations. DSGN-Target: {bare, data}. It indicates if the digital signature is calculated on the entire AMQP bare message ("bare") or only on the application-data section ("data"). DSGN-Signature: Base64 encoded digital signature.
		user-id AMQP Bare Message Standard property	Name-based UUID used to lookup sender's public key on the recipient side.
	Encrypted application-data section	**content-type** AMQP Bare Message Standard property	It shall be "***application/octet-stream***". Type/media type of the decrypted data shall be documented as part of the SWIM service design specification.
		footer section , key=**ENPT**	value = semicolon ***Encryption-Algorithm*** and **Encryption-Secret**. Symmetric Encryption algorithm identifier should be in accordance with RFC 3370. Different conventions should be documented. In all the cases, the selected algorithm must comply with applicable security policies, best practices and regulations. Encryption-Secret: optional field containing one or more comma separated "uuid" and "secret" pairs. For each intended recipient a colon separated "uuid" and "secret" pair is

Message level security mechanism	Applicable standards	AMQP annotated message section(s)	Restricted use
			provided. The uuid is the name-based UUID of the recipient and the "secret" is the symmetric key encrypted with the recipient's public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The "uuid" and "secret" pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e. publication messages) a mechanism should be put in place in order to allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid" and "secret" pairs in accordance with active subscribers' UUIDs. Taking into account the potential number of recipients, the full set of "uuid" and "secret" pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.

Table 55: Purple Profile message level security information distribution

For subscription management request and response messages (§4.2.2.2.1.2), *security information detached from the data* mechanism is used. In particular both request and response messages are signed (no message level confidentiality needs have been identified).

4.2.2.3.4 Non-nominal security cases

Mutual transport level authentication could fail if specific non-nominal events occur:

a. The X.509v3 certificate of one of the peer has been revoked.

b. The X.509v3 certificate of one of the peer expired.

c. The CRLs expired and it is not possible to renew it (e.g. CDP is not reachable).

d. The OCSP responder is not available because restarting or network failures.

As anticipated above, CRLs and X.509v3 maintenance activities should be properly planned in order to avoid, especially on the aircraft side, that certificates and/or CRLs expire while flying.

However above mentioned events could occur. For mitigating events *c* and *d* the Purple Profile requires advanced capabilities (Table 56) on the Air and Ground SWIM Nodes side and Purple Profile enabled applications side as well.

Capability	Description
OCSP responder URIs	It allows to try more than one URI when attempting to check the certificate revocation status via OCSP. OCSP URIs could be provided directly as extension of the X.509v3 certificate and/or configured locally on the OCSP requestor side.
CDP URIs	It allows to try more than one URI when attempting to download CRLs. CDP URIs could be provided directly as extension of the X.509v3 certificate and/or configured locally.
OCSP – CRL preference	It allows to configure the preference when OCSP and CRLs are both used: - OCSP preferred, CRLs as fallback. - CRLs preferred, OCSP as fallback.
OCSP – CRL Fallback	It allows to enable/disable fallback of the revocation status mechanisms.
Revocation check in case of network errors	It allows to indicate if the revocation check has to succeed in case CDPs and OCSP are not reachable because network errors.

Table 56: OCSP and CRL related non-nominal cases

For what concerns events *a* and *b*, different mechanism (modes) could be defined:

- Secure mode: the authentication fails. Alternative means for sharing the information may be used when needed until X.509v3 certificate is renewed or a new one is issued.
- Safe mode: the security constraints are less strong for a limited period of time. This is typically only allowed when the non-nominal case concerns the client's certificate:
  - Server only authentication (only applicable when it is the client's certificate that is revoked/expired). Transport level confidentiality and integrity are still protected.
  - Mutual authentication with alternative client's digital identity (transport level confidentiality and integrity are still protected):
    - Client is authenticated via username/password.
    - Server is authenticated via X.509v3 certificate.

This specification aims at describing the Purple Profile for advisory information sharing: taking into account the non-safety-related information, it has been considered not necessary to detail the safe-mode (the default mode is "secure"). Depending on the specific Purple Profile enabled SWIM service analysis and design ad-hoc safe mode could be defined and configured at Air and Ground SWIM Nodes level.

4.2.2.3.5 Cross-cutting security design considerations

In this section additional cross-cutting design considerations are provided as introduction to requirements in §4.3.5.

4.2.2.3.5.1 RBAC for administrative interfaces

Air and Ground SWIM Nodes configurations, policies and messaging resources are managed via administrative interfaces. Role based access control (RBAC) will be in place to grant access to administrative interfaces.

4.2.2.3.5.2 Time synchronization

Time synchronization is a must to have for all the security functions and also for reliability purposes. The Purple Profile does not constrain how the time is synchronized. The Purple Profile requires that for the Air and Ground SWIM Nodes and Purple Profile enabled applications (air and ground):

- the Coordinated Universal Time (UTC) time zone is used,
- with an accuracy of 1 second.

4.2.2.3.5.3 Domain Name System Security (DNSSEC)

Local (LAN), enterprise level and public Domain Name Systems (DNSs) could be used for names resolution when addressing specific networked resource (message queue, OCSP, etc.). This may introduce vulnerabilities that are mitigated via the advanced and optional use of Domain Name System Security (DNSSEC): it extends the DNS standard by providing the resolvers with origin authentication and integrity of DNS data.

4.2.2.4 Communication Network infrastructure

The network infrastructure will provide the following capabilities to the Purple Profile SWIM Nodes and Purple Profile enabled applications:

- End System support, i.e. TCP users
- IP routing
- Class of Service (CoS) – only A/G Network.
- Support for multilink (only A/G Network).
- Segregation of data from different aircraft domains.

The three networks can optionally support either IPv4 or IPv6 bindings. There is no requirement for all the networks to support the same bindings. The Aircraft can support either IPv4 or IPv6 bindings but not in the AISD on the same aircraft. The A/G network will support both binding to handle all aircraft. The Ground SWIM Enabled Application could support either IPv4 or IPv6 bindings but probably not both. The G/G network will support both binding to handle all applications. An example scenario is where Aircraft SWIM Enabled Application to Air PP SWIM Node connection uses IPv4, an Air PP SWIM Node to Ground PP SWIM Node connection uses IPv6 and a Ground PP SWIM Node to Ground SWIM Enabled Application connection uses IPv4.

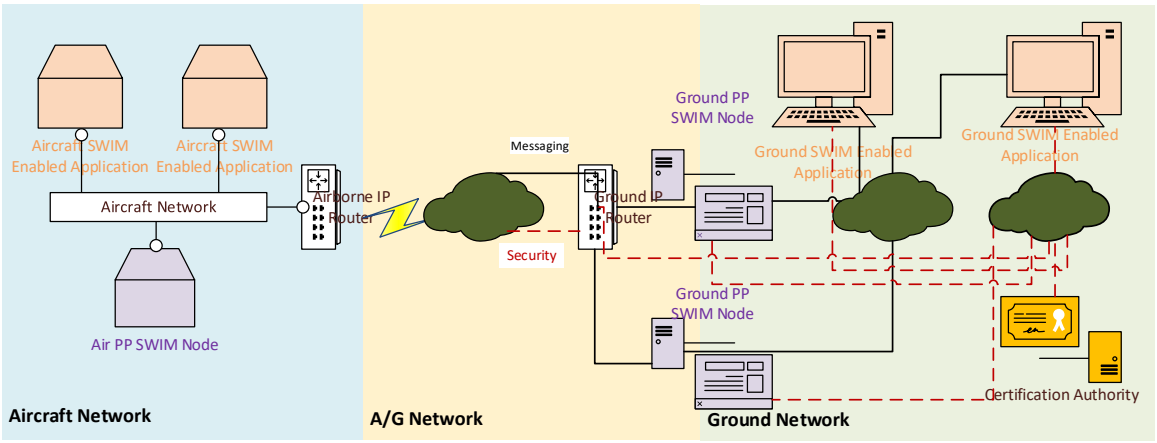


Figure 40: Communications Network Infrastructure

Current aircraft support IPv4 in the AISD in accordance with ARINC 821. It is expected that in the future aircraft will replace IPv4 with IPv6. It is never expected that an aircraft will support both IPv4 and IPv6 at the same time. Taking into account that there will be aircraft equipped with IPv4 and others with IPv6, the A/G Communications and the G/G Communications network infrastructures must support both IPv4 and IPv6. All TCP communication will be initiated by the aircraft for security reasons.

Note: Figure 40 shows the Aircraft SWIM enabled applications and the Air Purple Profile SWIM node on separate hosts but they can be on the same host, e.g. EFB. In this case, they won't need to communicate via the aircraft network.

The role of the CoS is to provide the communication system with the level of performance that is expected by the application in order to achieve its QoS requirements. When a network experiences congestion and delay, some packets must be prioritized to avoid random loss of data. CoS accomplishes this prioritization by dividing similar types of traffic into classes. It can be anticipated that for certain applications it will be necessary to prioritize messages. This would require the network to have more than 1 CoS associated with SWIM.

4.2.2.4.1 A/G Communication Network Infrastructure

The A/G Communication Network Infrastructure supports Purple Profile communication between Aircraft and Ground Purple Profile SWIM Nodes. The A/G network defined in this specification includes the datalinks' connection on the aircraft, the communications service provider(CSP) network and the ground domain network. The ground domain network connects to the CSP networks and is where the Ground Purple Profile SWIM Node is located. The A/G network needs to allow the following data to be exchanged between an IP router on the aircraft and an IP router on the ground:

1. Aircraft SWIM Enabled application data.
2. SWIM-TI protocol data to/from Air Purple Profile SWIM Node from/to Ground Purple Profile SWIM node.
3. Ground OCSPs and CDPs.

The A/G network needs to support the following capabilities:

- Routing the SWIM data from the IP router on the Aircraft Information Network to an IP Router on the G/G network and vice-versa over available datalinks. The A/G communication network infrastructure may contain multiple A/G and G/G routers.
- Segregation of data from different aircraft domains, if required. The aircraft data domains are described in §4.2.2.1.
- Support for multilink. The A/G network will provide a mechanism for SWIM data to be transferred over multiple datalinks which meet the SWIM data QoS requirements.

The Air/Ground Communication Network Infrastructure for SWIM services can be provided for example by the FCI or public networks such as LTE and GSM. Cabin based networks operated over TWLU and/or CWLU are out of scope for the SWIM Purple Profile.

Though the details of the Air/Ground communication network are out of scope for the SWIM Purple Profile, this technical specification includes requirements allocated to the communication network identified according to Purple Profile technical and non-functional requirements.

4.2.2.4.2 G/G Communication Network Infrastructure

From a network perspective the application layer resides on an end system. An End-to-End connection can be established over an internet of intermediate systems. The ground network must provide the connectivity from a Ground Purple Profile SWIM node to the following systems:

1. Ground IP router
2. Ground Purple Profile SWIM Enabled application
3. Certification Authority

4.2.2.4.3 Aircraft Information Network

The Aircraft SWIM Access Point is located in the AISD. The network must be built to provide the required connectivity and security taking the domain segregation restrictions into account.

The Aircraft Information Network is expected to be an IP network with an IP Router providing the interface to an A/G Communications Network Infrastructure which supports multiple links.

The Aircraft Information Network must provide the connectivity from the Air Purple Profile SWIM node to the following systems:

1. Aircraft SWIM Enabled application
2. Airborne IP router
3. (Optionally) local OCSP or/an CDPs.

4.2.2.5 Interface bindings

This section describes the rationale and the specificities on the interface bindings putting together messaging and security design aspects described in previous sections.

4.2.2.5.1 Network bindings

The capabilities provided by the three communication network infrastructures described in §4.2.2.4 are made available for Purple Profile SWIM Nodes and Purple Profile enabled applications via IP based bindings of <Network binding> type:

- Purple Profile <Service binding> and <Internal service binding> bindings are instantiated (stacked) over a <Network binding>. This allows bindings' client to access the bindings over the network.
- OCSP and CDP bindings are instantiated (stacked) over a <Network binding>. This allows Purple Profile enabled applications and SWIM Nodes to access the bindings over the network.

The bindings of <Network binding> type are specified in §4.3.7.

4.2.2.5.2 Purple Profile enabled SWIM Services bindings

As introduced in §3.1.1.2 and further detailed in §4.2.2.2.1 Purple Profile enabled SWIM services are made accessible to the application layer (Purple Profile enabled SWIM applications) via a pair of bindings of type <Service binding> federated via a binding of type <Internal service binding>.

Based on the analysed technical use cases, following bindings have been defined:

- (bindings triad) Purple Profile enabled SWIM service over FDRR-MEP/FDRMR-MEP:
    - Request and Response Message queues are made available (message distribution function described in §4.2.2.2.1.1) via two "*Fully decoupled Request/Response over AMQP*" <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network, §4.2.2.4.3) and another on the ground side (stacked with <Network binding> over the G/G Communication Network, §4.2.2.4.2). These two bindings are specified in this specification and they have to be instantiated according to the specific service (refer to the "contract" field) and directly accessed by SWIM enabled applications depending on the role (requestor, responder).
    - Airborne and Ground <Service binding> message queues are federated via "*Request/Response over AMQP federation*" <Internal service binding> (stacked with <Network binding> over the A/G Communication Network, §4.2.2.4.1) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding is specified in this specification and instantiated according to routing and segregation needs documented for each service (refer to §4.2.2.2.1).
- (bindings triad) Purple Profile enabled SWIM service over PS*-MEP:
    - Message topics and subscription handler are made available (message distribution and subscription management functions described in §4.2.2.2.1.2) via two "*Publish/Subscribe over AMQP*" <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network, §4.2.2.4.3) and another on the ground side (stacked with <Network binding> over the G/G Communication Network, §4.2.2.4.2). These bindings are specified in this specification and they have to be instantiated according to the specific service (refer to the "contract" field) and directly accessed by SWIM enabled applications depending on the role (publisher, subscriber). *Publication Registration Management* function (§4.2.2.2.1.2), when needed, it is realized via off-line exchange (e.g. SLA agreement and configuration) and not over <Service binding>.
    - Airborne and Ground <Service binding> message topics and subscription handlers are federated via "*Publish/Subscribe over AMQP federation*" <Internal service

binding> (stacked with <Network binding> over the A/G Communication Network, §4.2.2.4.1) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding is specified in this specification and instantiated according to routing and segregation needs documented for each service (refer to §4.2.2.2.1).

The "*Fully decoupled Request/Response over AMQP*" <Service binding> is described in Table 57 and specified (requirements) in §4.3.7. AMQP Message structure & format constraints are described in dedicated tables.

Binding section	Binding sub-section	Definition
Protocol stack	Stacking	Request/Response Messaging Entities Purple Profile Messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}.
	MEPs	The binding natively provides request and response messages distribution for the federated FDRR-MEP and FDRMR-MEP.
	Operations	AMQP 1.0 connection, session and link are initiated by the AMQP peer using an instance of this binding. Sending request or response message: - Sender entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with "source" link type (link type on the MQ side is "target"). Receiving request or response message: - Receiver entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with "target" link type (link type on the MQ side is "source").
	Message structure& format	The AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: - one header section. - one properties section. - one application-data section (body) consists of one data section or a single amqp-value section. - zero or one footer section.
	Fault/failure/error	In accordance with AMQP 1.0 core.
	Constraints	- Additional messaging functionalities are required on top of AMQP 1.0 core to fulfil Purple Profile design. - TLS 1.3 (amqps form only) is required but fallback to 1.2 is allowed. - The binding can be instantiated over IPv4 or IPv6. - AMQP 1.0 core transactions are not used. - Fixed range for the idle-time-out parameter of the AMQP open performative - The binding constrains the sections of the AMQP 1.0 annotated message. - The binding is instantiated and configured according to the elements described in the contract section. - AMQP 1.0 core filter restricted to http://www.amqp.org/specification/1.0/filters, APACHE.ORG:SELECTOR capability.
Security	Authentication	Point to point: mutual transport level authentication of AMQP 1.0 peers through TLS {1.2|1.3} according to the amqps form only. End to end: the binding provides mechanisms to transfer message level security information

Binding section	Binding sub-section	Definition
		from the sender and the intended recipient(s).
	Authorisation	Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the binding. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Integrity	Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Confidentiality	Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Non-repudiation	Point to point: audit logging. End to end: depending on the message level security controls used by the specific service.
QoS	Delivery guarantees	The binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile.
	Lifetime	Message with specified lifespan and Non-Temporary Queue.
	Durability	When not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message queues are supported.
	Ordering guarantees	{FIFO | Best effort message priority} message ordering guarantees are provided.
	CoSs	The instantiation of this binding allows to assign a specific class of service.
Contract	Addressing	The binding does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for request and response message queues.
	Messaging resources	Message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of message queues.
	Messaging Policies	Messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation.
	Security Policies	Security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured.
	QoSs	The instantiation of this binding requires that the applicable QoSs are documented and configured.
	CoS	The instantiation of this binding requires that the applicable CoS is documented and configured.
	Application-data	Although it is opaque for the binding, in order to enabled end to end interoperability the physical information model (e.g. JSON schema, XSDs, etc.) has to be documented.
	Application properties	The binding can use these properties for filtering and routing purposes. However, even if not used by the binding, in order to enabled end to end interoperability any application properties have to be documented.
Binding relationships	*Stacked* with <Network binding>	Binding instances are stacked with {IPv4 | IPv6} <Network binding>. Aircraft side binding instances are stacked with <Network binding> over the Aircraft Information Network. Ground side are stacked with <Network binding> over the G/G Communication Network.

Company General Use

Binding section	Binding sub-section	Definition
	Relies on Request/Response over AMQP federation <Internal service binding>	The binding relies on Request/Response over AMQP federation bindings for MEP federation.
	(optionally) *Relies on* CDP and/or OCSP bindings	The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.

Table 57: Fully decoupled Request/Response over AMQP binding

The "*Request/Response over AMQP federation*" <Internal Service binding> is described in Table 58 and specified (requirements) in §4.3.7. AMQP Message structure& format constraints are described in dedicated tables.

Binding section	Binding sub-section	Definition
Protocol stack	Stacking	Request/Response Messaging Entities Purple Profile Messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}.
	MEPs	The binding natively provides request and response messages distribution for the federated FDRR-MEP and FDRMR-MEP.
	Operations	AMQP 1.0 connection, session and link are initiated by the AMQP peer (i.e. Air SWIM Node) using an instance of this binding. Sending request or response message: - Sender entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with "source" link type (link type on the MQ side is "target"). Receiving request or response message: - Receiver entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with "target" link type (link type on the MQ side is "source").
	Message structure& format	The AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: - header, properties, application-data and footer from federated Fully decoupled Request/Response over AMQP binding instance. - one message-annotations section in case on-the-fly compression is enabled/provided.
	Fault/failure/error	In accordance with AMQP 1.0 core.
	Constraints	Same as Fully decoupled Request/Response over AMQP binding.
Security	Authentication	Point to point: mutual transport level authentication of AMQP 1.0 peers (Air and ground SWIM Nodes) through TLS {1.2|1.3} according to the amqps form only. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Authorisation	Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the binding. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).

Binding section	Binding sub-section	Definition
	Integrity	Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Confidentiality	Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Non-repudiation	Point to point: audit logging. End to end: depending on the message level security controls used by the specific service.
QoS	Delivery guarantees	The binding provides At-Most-Once. Optionally, it provides { At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer (i.e. Air SWIM Node) "connecting" (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile.
	Lifetime	Message with specified lifespan and Non-Temporary Queue.
	Durability	When not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message queues are supported.
	Ordering guarantees	{FIFO | Best effort message priority} message ordering guarantees are provided.
	CoSs	The instantiation of this binding allows to assign a specific class of service.
Contract	Addressing	The binding does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for request and response message queues.
	Messaging resources	Message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of message queues.
	Messaging Policies	Messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation.
	Security Policies	Security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured.
	QoSs	The instantiation of this binding requires that the applicable QoSs are documented and configured taking into account QoSs of federated Fully decoupled Request/Response over AMQP binding instances.
	CoS	The instantiation of this binding requires that the applicable CoS is documented and configured taking into account CoS of the federated Fully decoupled Request/Response over AMQP binding instances.
Binding relationships	*Stacked* with <Network binding>	Binding instances are stacked with {IPv4 | IPv6} <Network binding> over the A/G Communication Network.
	Federates Fully decoupled Request/Response over AMQP binding <Service binding>	The binding provides messaging functionalities aiming at federating Fully decoupled Request/Response over AMQP binding <Service binding> bindings pair(s).
	(optionally) *Relies on* CDP and/or OCSP bindings	The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.

Table 58: Request/Response over AMQP federation binding

The "*Publish/Subscribe over AMQP*" <Service binding> is described in Table 59 and specified (requirements) in §4.3.7. AMQP Message structure& format constraints are described in dedicated tables.

Binding section	Binding sub-section	Definition
Protocol stack	Stacking	Publish/Subscribe Messaging Entities Purple Profile Messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}.
	MEPs	The binding natively provides publication message distribution and subscription management for the federated PSPUSH-MEP and PSPULL-MEP.
	Operations	AMQP 1.0 connection, session and link are initiated by the AMQP peer using an instance of this binding. Sending publication message/subscription management request message: - Sender entity establishes an AMQP 1.0 link with the MT/Subscription handler's request MQ made available by this binding with "source" link type (link type on the MT/Subscription handler's request MQ side is "target"). Receiving publication message/subscription management response message: - Receiver entity establishes an AMQP 1.0 link with the MT/Subscription management response MQ made available by this binding with "target" link type (link type on the MT/ Subscription management response MQ side is "source").
	Message structure& format	The AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: - one header section. - one properties section. - one application-data section (body) consists of one data section or a single amqp-value section. - zero or one footer section.
	Fault/failure/error	In accordance with AMQP 1.0 core.
	Constraints	- Additional messaging functionalities are required on top of AMQP 1.0 core to fulfil Purple Profile design. - TLS 1.3 (amqps form only) is required but fallback to 1.2 is allowed. - The binding can be instantiated over IPv4 or IPv6. - AMQP 1.0 core transactions are not used. - Fixed range for the idle-time-out parameter of the AMQP open performative - The binding constrains the sections of the AMQP 1.0 annotated message. - The binding is instantiated and configured according to the elements described in the contract section. - AMQP 1.0 core filter restricted to http://www.amqp.org/specification/1.0/filters, APACHE.ORG:SELECTOR capability.
Security	Authentication	Point to point: mutual transport level authentication of AMQP 1.0 peers through TLS {1.2|1.3} according to the amqps form only. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Authorisation	Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the

Binding section	Binding sub-section	Definition
		binding. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Integrity	Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Confidentiality	Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Non-repudiation	Point to point: audit logging. End to end: depending on the message level security controls used by the specific service.
QoS	Delivery guarantees	The binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile.
	Lifetime	Message with specified lifespan, Non-Temporary Topic, Non-Temporary Queue (Subscription management), subscription with unspecified lifetime and (optionally) subscription with specified lifetime.
	Durability	When not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message topics, {durable | non-durable } subscription and { volatile | durable} subscription handler are supported.
	Ordering guarantees	{FIFO | Best effort message priority} message ordering guarantees are provided.
	CoSs	The instantiation of this binding allows to assign a specific class of service.
Contract	Addressing	The binding does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for message topics and subscription management request and response message queues.
	Messaging resources	Message topics and subscription management message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of these resources.
	Messaging Policies	Messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation.
	Security Policies	Security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured.
	QoSs	The instantiation of this binding requires that the applicable QoSs are documented and configured.
	CoS	The instantiation of this binding requires that the applicable CoS is documented and configured.
	Application-data	Although it is opaque for the binding, in order to enabled end to end interoperability the physical information model (e.g. JSON schema, XSDs, etc.) for publication message has to be documented. Purple Profile provides XML schema for subscription management request and response messages.
	Application properties	The binding can use these properties for filtering and routing purposes. However, even if not used by the binding, in order to enabled end to end interoperability any application properties have to be documented.
Binding	*Stacked* with	Binding instances are stacked with {IPv4 | IPv6} <Network binding>. Aircraft side binding

Binding section	Binding sub-section	Definition
relationships	<Network binding>	instances are stacked with <Network binding> over the Aircraft Information Network. Ground side are stacked with <Network binding> over the G/G Communication Network.
	Relies on Publish/Subscribe over AMQP federation <Internal service binding>	The binding relies on Publish/Subscribe over AMQP federation bindings for MEP federation.
	(optionally) *Relies on* CDP and/or OCSP bindings	The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.

Table 59: Publish/Subscribe over AMQP binding

The "*Publish/Subscribe over AMQP federation*" <Internal Service binding> is described in Table 60 and specified (requirements) in §4.3.7. AMQP Message structure& format constraints are described in dedicated tables.

Binding section	Binding sub-section	Definition
Protocol stack	Stacking	Publish/Subscribe Messaging Entities Purple Profile Messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}.
	MEPs	The binding natively provides publication message distribution and subscription management for the federated PSPUSH-MEP and PSPULL-MEP.
	Operations	AMQP 1.0 connection, session and link are initiated by the AMQP peer (i.e. Air SWIM Node) using an instance of this binding. Sending publication message/subscription management request message: - Sender entity establishes an AMQP 1.0 link with the MT/Subscription handler's request MQ made available by this binding with "source" link type (link type on the MT/Subscription handler's request MQ side is "target"). Receiving publication message/subscription management response message: - Receiver entity establishes an AMQP 1.0 link with the MT/Subscription management response MQ made available by this binding with "target" link type (link type on the MT/ Subscription management response MQ side is "source").
	Message structure& format	The AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: - header, properties, application-data and footer from federated Publish/Subscribe over AMQP binding instance. - one message-annotations section in case on-the-fly compression is enabled/provided.
	Fault/failure/error	In accordance with AMQP 1.0 core.
	Constraints	Same as Publish/Subscribe over AMQP binding.
Security	Authentication	Point to point: mutual transport level authentication of AMQP 1.0 peers (Air and ground SWIM Nodes) through TLS {1.2|1.3} according to the amqps form only. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Authorisation	Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the

Binding section	Binding sub-section	Definition
		binding. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Integrity	Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Confidentiality	Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).
	Non-repudiation	Point to point: audit logging. End to end: depending on the message level security controls used by the specific service.
QoS	Delivery guarantees	The binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer (i.e. Air SWIM Node) ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile.
	Lifetime	Message with specified lifespan, Non-Temporary Topic, Non-Temporary Queue (Subscription management), subscription with unspecified lifetime and (optionally) subscription with specified lifetime.
	Durability	When not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message topics, {durable | non-durable } subscription and { volatile | durable} subscription handler are supported.
	Ordering guarantees	{FIFO | Best effort message priority} message ordering guarantees are provided.
	CoSs	The instantiation of this binding allows to assign a specific class of service.
Contract	Addressing	The binding does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for message topics and subscription management request and response message queues.
	Messaging resources	Message topics and subscription management message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of these resources.
	Messaging Policies	Messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation.
	Security Policies	Security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured.
	QoSs	The instantiation of this binding requires that the applicable QoSs are documented and configured taking into account QoSs of federated Publish/Subscribe over AMQP binding instances.
	CoS	The instantiation of this binding requires that the applicable CoS is documented and configured taking into account CoS of the federated Publish/Subscribe over AMQP binding instances.
Binding relationships	*Stacked* with <Network binding>	Binding instances are stacked with {IPv4 | IPv6} <Network binding> over the A/G Communication Network.
	Federates Publish/Subscribe over AMQP binding <Service	The binding provides messaging functionalities aiming at federating Publish/Subscribe over AMQP binding <Service binding> bindings pair(s).

Binding section	Binding sub-section	Definition
	binding>	
	(optionally) *Relies on* CDP and/or OCSP bindings	The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.

Table 60: Publish/Subscribe over AMQP federation binding

All the above bindings are constrained in terms of required AMQP 1.0 annotated message sections and their use. The Purple profile constraints are described in the following tables.

AMQP 1.0 annotated message section	AMQP 1.0 annotated message section field	Purple Profile constraints
Header (mandatory)	**durable**	Set to true when durable message durability QoS is used.
	priority	Integer (min inclusive value = 0, max inclusive value = 9, default priority = 4).
	ttl	Mandatory and added by message producer. It is the lifespan relative to the message creation time property.
	first-acquirer	Not used. This field must be ignored.
	delivery-count	Used and mandatory to discover maximum number of retries.

Table 61: AMQP 1.0 annotated message Header section

AMQP 1.0 annotated message section	Key	Value	Purple Profile constraints
Zero or one delivery-annotations	-	-	The Purple Profile does not constrain this section. Purple Profile enabled services may use this section.
Zero or one message-annotations	**x-ontheflycompressed**	**{gzip|deflate}**	The message-annotations section is required when the on-the-fly QoS is configured at SWIM-TI level. One annotation is defined: it indicates that the payload (Bare Message Application Data) has been compressed on the fly by a distribution node. In accordance with AMQP 1.0 core, on receiving this annotation key, if not supported the receiving AMQP container MUST detach the link with a not-implemented error. However this should never occur because all the messaging resources and capabilities are agreed and configured in advance. The value indicates the compression algorithm used.

Table 62: AMQP 1.0 annotated message delivery and message annotation sections

AMQP 1.0 annotated message section	AMQP 1.0 annotated message section field	Purple Profile constraints
properties	**message-id**	UUID variant 2 version 4 (random) as defined in the IETF RFC 4122.

AMQP 1.0 annotated message section	AMQP 1.0 annotated message section field	Purple Profile constraints
(mandatory)	**user-id**	Message producer's Name-Based UUID as defined in the IETF RFC 4122. In the current Purple Profile specification, name-based UUIDs are derived/generated as follows: - Name: the X.500 Distinguished Names (DNs) from the entity's X.509v3 certificate. - Namespace: X.500 DN with namespace UUID "6ba7b814-9dad-11d1-80b4-00c04fd430c8" (IETF RFC 4122). It is assumed (refer to §6) that when moving to the SESAR industrialization/deployment phase, a governed registry will be available and maintained.
	to	Required, to be used in accordance with AMQP 1.0 core but the Purple Profile does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). This has to be documented as part of the binding's contract. Purple Profile implementations may use addresses syntax and semantics described in the latest working draft for OASIS AMQP Addressing (most of the AMQP 1.0 implementations support those schemes).
	subject	Require and to be used in accordance with AMQP 1.0 core. The Purple Profile does not constrain nor standardise the template (syntax, semantics) for the subject string for publication, request and response messages. The Purple Profile messaging can use this section for (e.g.) filtering and routing purposes. The syntax and semantics have to be documented as part of the binding's contract. The Purple profile standardises the subjects to be used for subscription management request and response messages.
	reply-to	Required for request messages only (including subscription management), to be used in accordance with AMQP 1.0 core but the Purple Profile does not constrain nor standardise the AMQP 1.0 core addressing scheme(s). This has to be documented as part of the binding's contract. Purple Profile implementations may use addresses syntax and semantics described in the latest working draft for OASIS AMQP Addressing (most of the AMQP 1.0 implementations support those schemes).
	correlation-id	UUID variant 2 version 4 (random) as defined in the IETF RFC 4122. Required for response messages only (including subscription management) and it represents the message-id of correlated (request) message.
	content-type	Required and to be used in accordance with AMQP 1.0 core. The Purple Profile does constrain this field: it must be set to the selected IETF RFC 2046 MIME Media type. Furthermore, the Purple profile standardises the content-type to be used for subscription management request and response messages: it must be "*application/xml*".
	content-encoding	To be used in accordance with AMQP 1.0 core and interpreted as per section 3.5 of IETF RFC 2616. In particular, it is used in combination with content type property and it indicates the compression standards used to compress original media type. Allowed encoding (refer to HTTP Content Coding Registry) are: - "gzip": GZIP (IETF RFC 1952) compressed original MIME type. - "deflate": Deflate (IETF RFC 1951) compressed original MIME type inside the zlib data format (IETF RFC 1950). Purple profile subscription management request and response messages are not compressed.
	absolute-expiry-time	The absolute point in time when the message is considered expired. Restricted to milliseconds since the Unix Epoch.
	creation-time	The absolute point in time when the message was created. Restricted to milliseconds since the Unix Epoch.

AMQP 1.0 annotated message section	AMQP 1.0 annotated message section field	Purple Profile constraints
	group-id	Not used. This field must be ignored.
	group-sequence	Not used. This field must be ignored.
	reply-to-group-id	Not used. This field must be ignored.
Zero or one application-properties	**AMQP map**	The Purple Profile does not constrain this section. Purple Profile enabled services may use this section. Purple Profile messaging can use this section for filtering and routing purposes. This is enabled and configured via messaging policies. Furthermore, this section is used when enforcing filtering criteria provided (if any) via subscription management messages (i.e. *Message Content* and *Producer Properties* selectors).

Table 63: AMQP 1.0 annotated message properties and application-properties sections

Message level security mechanism	Applicable standards	AMQP annotated message section(s) or/and field(s)	Restricted use
Security information attached to the data	XML Encryption, XML Signature	**content-type** AMQP Bare Message Standard property	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service design (e.g. application/xml for XML). It should be noticed that XML Encryption and XML Signature could be used also for non-XML data.
		AMQP Bare message application-data section	Not further restricted with respect to Purple Profile restrictions.
		Other sections and fields	Not further restricted with respect to Purple Profile restrictions.
	S/MIME 3.2 (RFC 5751)	**content-type** AMQP Bare Message Standard property	It must be set to the outer MIME type of the S/MIME message and only media types included in the S/MIME 3.2 chapter 3.9 are allowed.
		AMQP Bare message application-data section	The entire S/MIME message including all levels of nesting and wrapping shall be provided in a single AMQP Bare message application-data section. Constraints for backward compatibility with prior versions of S/MIME and constraints related to 7-bit transfer encoding are not applicable. Furthermore, as there are different ways to use S/MIME 3.2, further details have to be documented as part of the SWIM service design specification.
		Other sections and fields	Not further restricted with respect to Purple Profile restrictions.
	Any additional standard	AMQP Bare message	The use of the standard and additional restricted use of any AMQP Bare message sections shall be documented as part of the SWIM service design specification.
n d e t a	HMAC (RFC 2104)	**content-type** AMQP Bare Message Standard	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service

Company General Use

Message level security mechanism	Applicable standards	AMQP annotated message section(s) or/and field(s)	Restricted use
		property	design.
		footer	Purple Profile constrains the syntax and semantics.
		AMQP Bare message application-data section	Not further restricted with respect to Purple Profile restrictions.
		Other sections and fields	Not further restricted with respect to Purple Profile restrictions.
	Digital Signature	**content-type** AMQP Bare Message Standard property	Not restricted. It depends on the MIME type (RFC-2046) used and part of the SWIM service design.
		footer	Purple Profile constrains the syntax and semantics.
		AMQP Bare message application-data section	Not further restricted with respect to Purple Profile restrictions.
		Other sections and fields	Not further restricted with respect to Purple Profile restrictions.
	Encrypted application-data section	**content-type** AMQP Bare Message Standard property	It shall be "***application/octet-stream***". Type/media type of the decrypted data shall be documented as part of the SWIM service design specification.
		footer	Purple Profile constrains the syntax and semantics.
		AMQP Bare message application-data section	Not further restricted with respect to Purple Profile restrictions.
		Other sections and fields	Not further restricted with respect to Purple Profile restrictions.

Table 64: AMQP 1.0 annotated message restrictions for message level security

Standards	Key	Value & Purple Profile constraints
HMAC footer entry	**HMAC**	value= semicolon separated ***HMAC-Algorithm***, ***HMAC-Target, HMAC-Digest*** *and* ***HMAC-Secret***. HMAC-Algorithm: HMAC cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations. HMAC-Target: {bare, data}. It indicates if the HMAC is calculated on the entire AMQP bare message ("bare") or only on the application-data section ("data"). HMAC-Digest: Base64 encoded message digest. HMAC-Secret: optional field containing one or more comma separated "uuid" and "secret" pairs. For each intended recipient a colon separated "uuid" and "secret" pair is provided. The uuid is the name-based UUID of the recipient and the "secret" is the symmetric key encrypted with the recipient's public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The "uuid" and "secret" pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e.

Standards	Key	Value & Purple Profile constraints
		publication messages) a mechanism should be put in place in order to allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid" and "secret" pairs in accordance with active subscribers' UUIDs. Taking into account the potential number of recipients, the full set of "uuid" and "secret" pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.
Digital Signature footer entry	**DSGN**	value= semicolon separated ***DSGN-Algorithm***, ***DSGN-Target*** and ***DSGN-Signature***. DSGN-Algorithm: Digital signature cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations DSGN-Target: {bare, data}. It indicates if the digital signature is calculated on the entire AMQP bare message ("bare") or only on the application-data section ("data"). DSGN-Signature: Base64 encoded digital signature.
Encrypted application-data section footer entry	**ENPT**	value = semicolon separated ***Encryption-Algorithm*** and **Encryption-Secret**. Symmetric Encryption algorithm identifier should be in accordance with RFC 3370. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations Encryption-Secret: optional field containing one or more comma separated "uuid" and "secret" pairs. For each intended recipient a colon separated "uuid" and "secret" pair is provided. The uuid is the name-based UUID of the recipient and the "secret" is the symmetric key encrypted with the recipient's public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The "uuid" and "secret" pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e. publication messages) a mechanism should be put in place in order to allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid" and "secret" pairs in accordance with active subscribers' UUIDs. Taking into account the potential number of recipients, the full set of "uuid" and "secret" pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.

Table 65: AMQP 1.0 annotated message footer restrictions

Message Type	AMQP 1.0 subject properties field values
SubscriptionRequest	https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRequest
SubscriptionResponse	https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionResponse
UnsubscriptionRequest	https://sesarju.eu/swim/PP/SubscriptionManagement:UnsubscriptionRequest
UnsubscriptionResponse	https://sesarju.eu/swim/PP/SubscriptionManagement:UnsubscriptionResponse
SubscriptionRenewRequest	https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRenewRequest

Message Type	AMQP 1.0 subject properties field values
SubscriptionRenewResponse	https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRenewResponse
UpdateSubscriptionFilterRequest	https://sesarju.eu/swim/PP/SubscriptionManagement:UpdateSubscriptionFilterRequest
UpdateSubscriptionFilterResponse	https://sesarju.eu/swim/PP/SubscriptionManagement:UpdateSubscriptionFilterResponse
ActiveSubscriptionsRequest	https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsRequest
ActiveSubscriptionsResponse	https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsResponse
ActiveSubscriptionsNotify	https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsNotify

Table 66: AMQP 1.0 subject properties field values for subscription management messages

4.2.2.5.3 Identity Management bindings

CDP and OCSP services analysed and discussed in §4.2.2.3 are used by Purple Profile enabled applications, Air SWIM Node and Ground SWIM Node through standard based interface bindings:

- OCSP binding has to be conformant with IETF RFC 6960. In particular OCSP over HTTP as described in the IETF RFC 6960 Appendix A is used.
- CRL distribution points:
  - HTTP CDP as defined in IETF RFC 2585.
  - LDAP CDP as defined in IETF RFC 4523.

At Purple Profile technical view level, these bindings are ground services:

- stacked with <Network binding> over the G/G Communication Network, §4.2.2.4.2, and
- accessible by Ground SWIM Nodes and ground Purple Profile enabled applications via G/G Communication Network,
- accessible (when supported and required – refer to the technical view) by Air SWIM Nodes and aircraft Purple Profile enabled applications via networking between A/G (§4.2.2.4.1) and G/G communication networks.

As anticipated in §4.2.2.3, specific avionics architecture deployment options may be evaluated and adopted for certificate revocation status check. In this case, the above bindings may be accessible by aircraft Purple Profile enabled applications and Air SWIM node via the Aircraft information network (i.e. one or more of those bindings are stacked with <Network binding> over the Aircraft information network, §4.2.2.4.3).

These bindings of <External service binding> type are specified in §4.3.7.

4.2.2.5.4 Interface with Aircraft systems

Data connectivity should be validated and verified to ensure non-interference and isolation from certified aircraft systems during data transmission and reception. Air PP SWIM Node is able to receive data from aircraft systems, but data transmission from Air PP SWIM Node to aircraft systems is actually not possible per EASA AMC20-25.

As a result, this calls for an ADIF compliant integration based on an A834 protocol allowing access to the following generic parameters:

AIR SWIM AP parameter	Aircraft Parameter	Units	Range	Resolution	Comment
Airborne status	WeightOnWheels	Discrete	0 = ground		
time	TimeGMT	Alphanumeric	HH:MM:SS.SS	0.01 s	Per ARINC 429
position	Latitude	Degrees	±180	0.000172	Per ARINC 429
	Longitude	Degrees	±180	0.000172	Per ARINC 429

Table 67: Minim set of avionics parameters used by the Air SWIM Node

Air PP SWIM Node/Access point is not designed to be directly operated by flight crew. These avionics system parameters purpose are:

- **Time (mandatory)**: The time reference for aviation is defined to be the Coordinated Universal Time (UTC), which is based on International Atomic Time. Time accuracy of data link communications utilized by air traffic services units, and clocks devices shall ensure correct time within 1 second of UTC[5].

  UTC time is the on-board reference for aeronautical operation supporting flight regularity, synchronised with ANSP time reference (synchronisation which is usually correlated with GNSS signals).

  Air PP SWIM Node internal time reference used for messaging time stamping should be aligned to this aviation time reference, which would require access to the on-board avionics clock data.

  Note: Although a single time source is sufficient for non-safety operations, a fall-back procedure may be needed at system level to support higher reliability. Such mechanisms may be already available for ADIF time reference parameter depending on the avionics source considered.

- **Airborne status (optional):** The flight phase is crucial for aeronautical operations, especially for critical phases of flight[6]. During such critical phases of flight, crew members shall not perform any activities other than those required for the safe operation of the aircraft.
  In addition, data communication performance and continuity may be affected during IN/OUT condition changes, and may depend on the surrounding aeronautical environment data communication capabilities.

  Air PP SWIM Node may implement some limitations, or adaptations due to the airborne or ground condition of the aeroplane. As a minimum, the aeroplane airborne status may be needed to achieve this purpose.

- **Position (optional)**: Commercial air transportation is operated worldwide. Depending on the ground deployment options, there may be non-centric topology of ground access points available, for which avionics system would have to choose from.

  One possible Air PP SWIM Node selection mechanism may be based on the aeroplane position in order to optimise messaging performance in term of latency, coping either with dedicated resources or dealing with systems' overloads.

4.2.2.6 Technical-Functional views traceability

This section provides (table format) the traceability between the "what" (functional viewpoint) and the "how" (technical viewpoint). Some aspects described in the "what" are not directly traced by the "how" because there are no interoperability needs. This has to be interpreted as described in the introduction of §4. Furthermore, at requirement level, the traceability between the "what" and the "how" (when applicable) is documented using the <SATISFIES> link [Appendix C].

---

5 This is the time reference accuracy for data communication in aviation, as addressed in ICAO Annexes 2, 10, 11 and 15, and regulated in standardized European rules of the Air, EC 2012-0923: 3401.

6 Annex I (Definitions) of the Regulation (EU) 965/2012 on Air Operations contains definitions for critical phases of flight, according to airplane types and operations, and standardized European rules of the Air, EC 2012-0923: 3401.

Concept/function	"What" to "How"
Messaging entities	Instantiation over AMQP 1.0 core of applicable messaging entities have been documented in the technical view.
Messaging QoS/characteristics	Instantiation over AMQP 1.0 core of applicable messaging characteristics/QoSs have been documented in the technical view.
Message distribution	Federated PSPUSH-MEP, PSPULL-MEP, FDRR-MEP and FDRMR-MEP MEPs over messaging capabilities on top of AMQP 1.0 core. The applicability of the latter is restricted in some area documented in the technical viewpoint. Furthermore, when instantiating the applicable MEPs (PSPUSH-MEP, PSPULL-MEP, FDRR-MEP and FDRMR-MEP) over the technical architecture, following constraints have to be taken into account: - Bi-directional message exchange over aircraft-initiated (TCP) connections. - Aircraft-initiated transport connectivity management (establishing, releasing, maintaining). - Store-and-forward mechanism to cope with temporary link unavailability (aircraft-ground Purple Profile interaction). - Messaging characterization statements of applicability to Purple Profile.
Message routing	Messaging capabilities on top of AMQP 1.0 core. The applicability of the latter is restricted in some area documented in the technical viewpoint. Furthermore, when instantiating the message routing over the technical architecture, following constraints have to be taken into account: - Aircraft data domains segregation. - Due to aviation configuration control rules (§4.2.2.1), aircraft side message routing policies cannot be dynamically defined/updated. - Messaging characterization statements of applicability to Purple Profile (e.g. context-based routing for non-nominal cases). The technical architecture relies on the message routing function to federate aircraft and ground side messaging. Finally, the AMQP 1.0 core addressing scheme(s) is not constrained nor standardized. Addressing scheme has to be documented together with non-opaque addressing for request and response message queues.

Message filtering	Messaging capabilities on top of AMQP 1.0 core. The applicability of the latter is restricted in some area documented in the technical viewpoint. Furthermore, when instantiating the message routing over the technical architecture, following constraints have to be taken into account: - Aircraft data domains segregation. - Due to aviation configuration control rules (§4.2.2.1), aircraft side message filtering policies cannot be dynamically defined/updated. - Messaging characterization statements of applicability to Purple Profile (e.g. context-based filtering for non-nominal cases). - In case of information uplink, in order to optimize the use of the aircraft and A/G network resources, the filtering should be enforced on the ground (ground side Purple Profile and/or Publisher/Responder side).
Message enrichment	In the Purple Profile, message enrichment is currently used only for on-the-fly compression. The “what” and “how” are described in the technical view.
Messaging policy management	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.
Authentication	Mutual transport level authentication of AMQP 1.0 peers through TLS 1.2 or TLS 1.3 according to the *amqps* form only.
Authorization	The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers).
Audit	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.
Confidentiality ensuring	Transport level confidentiality is provided through TLS 1.2/1.3 standard mechanisms.
Information Integrity and authenticity ensuring	Transport level integrity and authenticity are provided through TLS 1.2/1.3 standard mechanisms.
Message screening	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.
Overload protection	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.
Security Policy management	No technical interoperability needs have been recognized. The Purple Profile is not constraining the “how”. The functional view requirements concerning this function represent the reference for prototyping activities.

Table 68: Technical-Functional views traceability

4.2.3 Deployment View

The Purple Profile deployment viewpoint provides deployment options addressing the "where" in terms of architecture technical and integration options. It mainly addresses the concern about how to deploy the ("what" and "how" of) Purple Profile (technical view, §4.2.2).

General recommendations/principles about the deployment options [51]:

- *Deployment options should not break interoperability*,
- *Deployment options should not be in contradiction with documented design decisions and principles*,
- *If any additional requirement is needed to support such deployment option it shall be identified and specified*.

This specification does not impose/restrict the deployment options and the list of deployment options is not supposed to be complete and exhaustive.

4.2.3.1 Minimal avionics installation options

As the Air Purple Profile SWIM Node belongs to the Airline Information Service Domain (AISD), an insertion with minimum impact to certified avionics' equipment should be allocated to AISD avionics systems. Thus, integration targeting minor avionics impacts, as seen in §4.2.2.1, should potentially be mapped onto the actual avionics systems:

- **NSS**: ARINC 821 Network Server System, for Part 25 aircraft type supporting it, qualified against the aircraft's type certification.
  Core NSS equipment is the Network server unit (NSU) which can provide Air Purple Profile SWIM Node needed processing capability, memory, avionics interface with ACD, and with an IP Router.
- **EFB**: ARINC 828 Electronic Flight Bag System (EFB) supporting a wide variety of aircraft type, providing that its installation is qualified against EASA AMC 20-25 "Airworthiness and operational consideration for Electronic Flight Bags (EFBs)".

  Core EFB equipment is based on a pair of EFBPU which can provide Air Purple Profile SWIM Node needed processing capability, memory, along with an AID providing avionics interface with ACD and with an IP Router.

Assuming EFB level2 installation compliance (ADIF capable), there are several options for installing the Air PP SWIM AP on the EFB system: allocation to the EFBPU, allocation to the NSU, or allocation mixed between EFBPU and NSU.

4.2.3.1.1 Installation on EFBPU

As per EASA EU-OPS, portable electronic devices (PEDs) are any kind of electronic device brought on board the aircraft by crew members, passengers, or as part of the cargo and that are not included in the approved aircraft configuration. When PED have transmission capabilities, they are classified as T-PED. PED subject to administrative control by the operator, ensuring that no unauthorized changes are made to the hardware, software or databases, is classified as a C-PED.

Per EASA AMC20-25, EFB system may have both airworthiness and operational impacts depending on the category/type of EFB/application.

Company General Use

Airworthiness approval is necessary for installed EFB systems, as well as EFB installed resources and mounting device, whereas portable EFB device does not require an airworthiness approval but its presence and use in the cockpit needs to be operationally evaluated.

EFB operational software is classified under three categories (A, B, and C):

- Type A applications are EFB applications whose malfunction or misuse would have no adverse effect on the safety of any flight operation.
- Type B applications are EFB applications based on the severity of failure conditions resulting from malfunctions and misuse.
- Type C applications are EFB applications for which the severity of failure conditions is evaluated against EASA AMC20-25 guidelines.

According to the safety assessment provided in §4.2.2.1, **Air PP SWIM Node** software and user's application(s) must be **classified as** a **Type A** applications **installed on C-PEDs**.

One main issue with EFBPU installation choice is linked to cockpit side synchronisation of received information to ensure pilots awareness consistency. This implies that either there is a shared Air PP SWIM AP allocated to a single EFBPU, or that there are dual full or partial Air PP SWIM APs allocated to both EFBPU, as shown below:

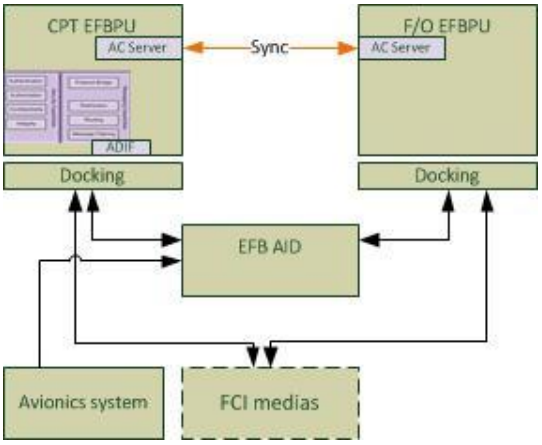


Figure 41: EFBPU installation and cockpit side synchronisation option 1

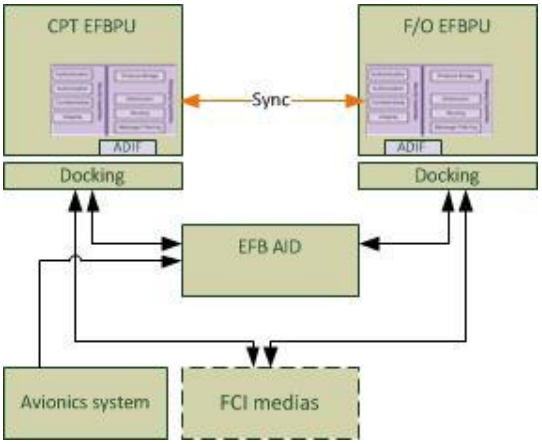


Figure 42: EFBPU installation and cockpit side synchronisation option 2

Both installations allow the Air PP SWIM AP(s) to get access to Aircraft generic parameters through the A834 ADIF interfaces.

The following table synthetises impacts of these installation choices:

Impacts	Single EFBPU	Dual EFBPU
Flight Crew	PP Operations are only accessible from one position at a time. Information is shared with F/O through Aircraft server applicative synchronisation.	PP Operations accessible from both positions. Any exchange of information may need to be synchronised so that pilots have the same situational awareness.
Access to AP	A/C Parameters are acquired on one side only.	A/C Parameters are acquired on both sides. Possible discrepancies due to avionics parameters latencies need to be evaluated.
Dispatch	One EFBPU holds all dispatch constraints; other side EFBPU is not an alternate able to support a degraded mode.	A/C SWIM capacities are redounded. Only dual failures may have an impact on SWIM based operation, provided a procedure for information synchronisation between pilots is available.
Connectivity	Only CPT EFB has FCI connectivity.	Both sides have FCI connectivity. This mandates FCI for a routing capability, either at commutation level (VLAN) or at routing level (IP router) allowing sharing FCI radio communication system.
Cyber security	Only EFB CPT shows an attack surface	Both EFBs are showing an attack surface.
PP architectures	This is a single Air PP SWIM Node for this A/C; where crew synchronisation requires a server above the PP SWIM AP upper interface.	Two Air PP SWIM Nodes, for which internal synchronisation will be required, which is not addressed under PP architecture.

Table 69: Impacts of EFBPU installation choices

4.2.3.1.2 Installation on NSU

NSU is avionics equipment attached to the Aircraft, and thus part of the TC configuration, it is therefore subject to all airworthiness constraints. It natively allows supporting ARINC 834 ADIF and connectivity interfaces. It also provides a single access point to avionics and open world for data communication and messaging, thus easing the cockpit information synchronisation.

This kind of installation is resumed in the following drawing:

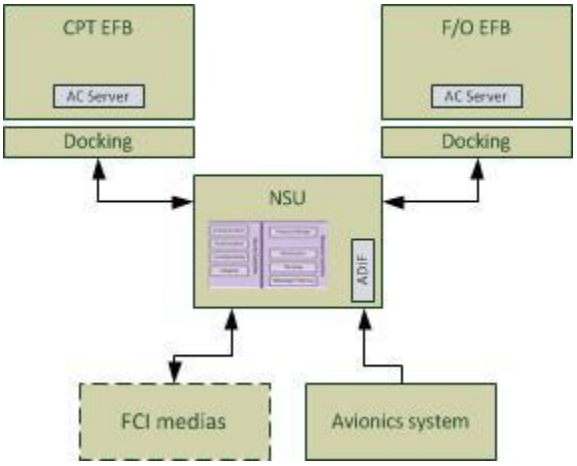


Figure 43: NSU installation

The following table synthetises impacts of this installation choice:

Impacts	NSU allocation
Flight Crew	Information exchanges are centralised within the NSU and distributed to both pilots' sides allowing a consistent situational awareness. Pilots have control on NSU (can enable/disable any time)
Access to AP	APs are acquired by the NSU. As such, updating/upgrading AP access is directly linked to the NSU configuration control, which must be done under operator's CAMO.
Dispatch	NSU is a single point of failure, for which there is no backup procedure possible. However, actual MMEL NSU categorisation does not impair A/C dispatch anyway.
Connectivity	NSU is natively designed to handle open wireless communications and is able to host the A/C open routing function. Any FCI needed upgrades can be isolated to this equipment.
Cyber security	NSU is under avionics controls, and thus not directly on an attack surface. NSU configuration is under operator's CAMO control.
PP architectures	This installation is consistent with PP architectures up to the NSU. NSU configuration is not dynamically upgradable, as being part of the A/C TC (thus any installed policies are static). NSU has no/few storing capabilities. NSU is not intended to be an End System (thus, is not expected to host PP enabled applications/services). NSU can implement radio-com preferences as a QoS mechanism.

Table 70: Impacts of NSU installation choice

4.2.3.1.3 Mix Installation of EFBPU & NSU

Possible allocation for Air Purple Profile SWIM Node may be for part of it to the NSU (which is natively designed for managing the aircraft open radio communications) and part of it to EFBPUs (which is natively designed for interfacing with pilots). Also, Air Purple Profile SWIM Node functions dependent of aircraft configuration would be best allocated to NSU, while functions dependent of aircraft operations would be best allocated to EFBPU.

An example of such kind of installation is resumed in the following drawing:

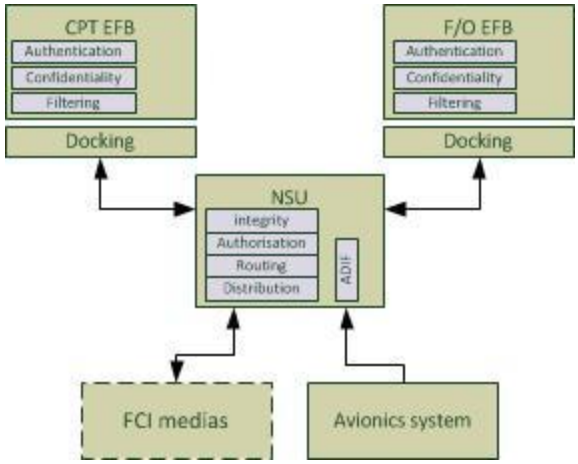


Figure 44: Mix Installation of EFBPU & NSU

The following table synthetises impacts of this installation choice:

Impacts	NSU	EFBPU(s)
Flight Crew	Information exchanges are centralised within the NSU.	Information is distributed to both pilots' sides allowing a consistent situational awareness. Each pilot can analyse the information on its position at its convenience with local filtering methods.
Access to AP	Air PP SWIM AP needed APs are acquired by the NSU. As such, updating/upgrading AP access is directly linked to the NSU configuration control, which must be done under operator's CAMO.	Applicative APs are acquired by the EFBPU according to the ADIF ICD built by the EFB system integrator. Air PP SWIM AP needed APs are not known to end users.
Dispatch	NSU is a single point of failure, for which there is no backup procedure possible.	End user accesses to Air PP SWIM AP are redounded. Only dual failures may have an impact on SWIM based operation, provided a procedure for information synchronisation between pilots is available.
Connectivity	NSU is natively designed to handle open wireless communications and is able to host the A/C open routing function. Any FCI needed upgrades can be isolated to this equipment.	T-PED potentially have connectivity (depending on wireless signals), but under this architecture would require a ground based NSU mirror to establish PP messaging according to such installation.

Cyber security	NSU is under avionics controls, and thus not directly on an attack surface. Thus NSU is indicated to host security CM related to network and radio medias controls.	EFBPU is dedicated to pilots and is under operator's EFB integrator responsibility.
PP architectures	NSU configuration is not dynamically upgradable, as being part of the A/C TC (thus any installed policies are static). NSU has no/few storing capabilities. NSU is not intended to be an End System (thus, is not expected to host PP enabled applications/services). NSU can implement radio-com preferences as a QoS mechanism.	EFBPU requiring a remote dynamic configuration should ensure this configuration mean is designed so that this capability can be approved under the operator maintenance process.

Table 71: Impacts of mix EFBPU & NSU installation choice

4.2.3.1.4 Installation options analysis

The following table addresses Air Purple Profile SWIM Node installation main impacts on aircraft airworthiness and operators' processes, according to the nature of Air Transport (AT) operations:

Impacts	Large A/C (AT mainline)	Small A/C (AT Regional)	Light A/C (AT bizjet)
A/C Airworthiness	Full or partial installation over NSS must be evaluated by the TC, or STC holder. Full or partial Installation over an existing EFB system should not impact A/C initial airworthiness.	Installation over an existing EFB system should not impact A/C initial airworthiness. Installation of a standard EFB system must be evaluated by the TC, or STC holder.	Installation of standard EFB system must be evaluated by the TC, or STC holder. Non-standard installation must be evaluated by the TC, or STC holder.
A/C Operator CAMO	Installation should not impact A/C MMEL. Update of NSU configuration management under operator Part M, or Part 145 may be evaluated.	Installation should not impact A/C MMEL. EFB configuration is under air transport certificate holder's EFB integrator responsibility.	Installation should not impact A/C MMEL. EFB configuration is under air transport certificate holder's EFB integrator responsibility.

Air Transport operator	Full or partial installation over NSS must be evaluated by air transport certificate holders. Full or partial installation over EFB must be evaluated by holders of ETSO authorisations covering EFB software applications against EASA AMC20-25, such as: • Assessment of aspects governing Crew Resource Management • Procedure in place to control configuration of the system • Procedure in place to ensure security against unauthorised intervention	Full or partial installation over EFB must be evaluated by holders of ETSO authorisations covering EFB software applications against EASA AMC20-25, such as: • Assessment of aspects governing Crew Resource Management • Procedure in place to control configuration of the system • Procedure in place to ensure security against unauthorised intervention	Full or partial installation over EFB must be evaluated by holders of ETSO authorisations covering EFB software applications against EASA AMC20-25, such as: • Assessment of aspects governing Crew Resource Management • Procedure in place to control configuration of the system • Procedure in place to ensure security against unauthorised intervention Portable EFB device presence and use in the cockpit needs to be evaluated.

Table 72: Air PP SWIM Node installation main impacts on aircraft airworthiness and operators' processes

4.2.3.2 Cardinality of the relationship between the Air PP SWIM Node and Ground PP SWIM Node

The PP design is based on the federation of messaging capabilities realized by proper messages distribution and routing between Air PP SWIM Node and Ground PP SWIM Node pair. Irrespective of failover and replication technical strategies for a given Ground PP SWIM Node, two main options have been envisaged for the cardinality of the relationship between the Air PP SWIM Node and Ground PP SWIM Node:

A. For all the PP Enabled SWIM services consumed and provided by a given aircraft, a single Ground PP SWIM Node is used. In terms of messaging, this requires that the Air PP SWIM Node is configured to always connect to that Ground PP SWIM Node irrespective of the service consumed/provided. In this case the Ground PP SWIM Node is recommended to be part of the concerning Civil AU Operations Centre.

B. For different PP Enabled SWIM services consumed and/or provided by a given aircraft different Ground PP SWIM Node are used. In terms of messaging, this requires that the Air PP SWIM Node routing is configured to connect to the ground PP SWIM Node assigned to the specific consumed/provided service. A possible variant of this option is that for aircraft provided services the deployment option A is applied. In this case, deployment option B applies only to services consumed by the aircraft.

4.2.3.3 Deployment options for response message queues (PPUC-01 and PPUC-03)

Following deployment options have been identified in the technical view §4.2.2.2.1:

1. PPUC-01 (a and b): ground side response message queue allowing the Ground PP SWIM Node to receive response messages for the ground SWIM service is a messaging resource that could be part of the service provider or Ground PP SWIM Node messaging.

2. PPUC-03 (a and b): ground side response message queue allowing ground applications to receive response messages is a messaging resource that could be part of the requestor or Ground PP SWIM Node messaging.

4.2.3.4 Identity management deployment

As described in §4.2.2.3.1, the Purple Profile security technical view is based on the adoption of constrained set of cryptographic keys and algorithms and on the X.509 version 3 certificates as digital identity type. X.509v3 certificates and cryptographic keys are managed via Public Key Infrastructure (PKI) that encompasses administrative procedures and local and remote resources and services. Furthermore, in the Aviation domain a number of regulations and standards exist to properly manage Aviation cybersecurity.

The Purple Profile is not responsible for defining and/or identifying applicable regulations and procedures: without being exhaustive and complete, applicable regulations and standards have been considered and referred to by requirements.

Public Key Infrastructure (PKI) consists of a set of standards, procedures, software, and people for implementing authentication/authenticity, authorization, confidentiality and integrity using public key cryptography. In particular the PKI provides the means for requesting, installing, configuring, validating, managing and revoking X.509 certificates used for digital signature, encryption, authentication and authorization (Attribute Based Access Control supported by X.509 certificate attributes).

Within the PKI, the Certification Authority (CA) is responsible for creating, signing, emitting and maintaining X.509 certificates and revocation lists (CRL). In particular the CA covers three main functions:

- The Certificate Management that issues certificates and maintains certificates revocation lists.
- The Registration Authority (RA) is the administrative function in charge of registration of entities in the Public Key Infrastructure (PKI).
- The Validation Authority (VA) is the function in charge of validation of the certificates.

The technical view refers in general to CA irrespective of possible deployment options such as the Bridge CA and CA delegation (or hierarchical PKI). At technical level, the CA provides capabilities used by the Purple Profile enabled applications and SWIM Nodes irrespective of how the trust-relationship between subordinate CAs and/or root CAs is established.

Although additional ones could be identified, basic options are documented in the SESAR 1 TAD §2.4.2.1.1 [51]: they are mainly Bridge CA and CA delegation (or hierarchical PKI).

As documented in §4.2.2.3.1, typically for all the security infrastructure based on PKI, there are protected stores at infrastructure level used to store X.509 certificates, keys, CRLs and trusted certificates. These stores could also not be at infrastructure layer: concerned enterprises, are not forced to create SWIM specific stores, when the capability is available, it is recommended to reuse it. This is especially relevant for the aircraft where potentially several entities need to access and to check X.509 related information using on-board already available store capabilities.

A possible option providing concerned aircraft components with a consistent access to these information (e.g. avoid duplication of stores/CRLs) could be to have a local (i.e. on-board) trusted OCSP responder: aircraft applications and Air SWIM Node use this local OCSP responder to check the

status of certificates. The OCSP relies on local store(s) subject to maintenance and updates (e.g. CDPs). This is only an illustrative example: the Purple Profile is not responsible for the complete aircraft architecture and it is not mandating any specific deployment option.

4.3 Functional and non-Functional Requirements

In this section the SWIM Purple Profile technical systems requirements are provided. The requirements breakdown is based on requirements types and architecture views (§4.2):

Functional view (§4.2.1):

- §4.3.1 provides functional requirements. These requirements concern the "what" the Purple Profile may/could/shall do. When applicable, functional requirements provided in this section are "satisfied" by requirements in the technical view (§4.3.2 to §4.3.7).

Technical view (§4.2.2):

- §4.3.2 provides design and construction constraints requirements.
- §4.3.3 provides reliability requirements concerning the robustness to abnormal operating conditions.
- §4.3.4 covers performance characteristics and in particular it provides requirements concerning capacity, accuracy, timing performances, software resource usage, etc.
- §4.3.5 provides security and privacy requirements, including access limitations, data protection and recovery methods. Requirements included in this section are security requirements applicable to the Purple Profile or/and to the specific technical functions (e.g. Messaging).
- §4.3.6 provides safety requirements.
- §4.3.7 provides interface requirements including the specification of the interfaces bindings.

Purple Profile requirements are based on an extended template (which respect to programme level template) described in Appendix C.

4.3.1 Capabilities (functional view)

This section provides the requirements concerning the Purple Profile functional view (§4.2.1). These requirements address the concern about what the Purple Profile technical systems shall/should/could do (Purple Profile functional viewpoint).

These functional requirements are grouped in accordance with the SWIM-TI functional decomposition (functional blocks and functional blocks' functions) described in EATMA. It is a logical grouping of functions describing what the Purple Profile technical systems do.

4.3.1.1 Messaging

This section provided messaging requirements concerning the functional view. Requirements have been grouped per messaging function.

4.3.1.1.1 Messaging-distribution

[REQ]

Identifier	REQ-17.01-TS-0010.0005
Title	Support of Publish/Subscribe Push Message Exchange Pattern

Requirement	The SWIM-TI Messaging shall provide the Push style Publish/Subscribe Message Exchange Pattern (PSPUSH-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEPs). The Publish/Subscribe Push is one of the identified MEPs needed to enable the exchanging of information between ATM participants. An unique identifier of this MEP has been defined: PSPUSH-MEP. The PSPUSH-MEP is characterized as follows: - Conversation direction: 1 way (Publisher-> Consumer) - Cardinality: many-many - Decoupling: Time decoupling; Space decoupling, Synchronization decoupling. The main difference with respect to the other MEPs is the support of full time, space and synchronization decoupling. This characterization is further detailed as part of the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities, events and QoS concerning applicable to this MEP. In particular the entities concerning this MEP are Message Topic, Intermediary, Publisher, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0010
Title	Support of Publish/Subscribe Pull Message Exchange Pattern
Requirement	The SWIM-TI Messaging shall provide the Pull style Publish/Subscribe Message Exchange Pattern (PSPULL-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEPs). The Publish/Subscribe Pull is one of the identified MEPs needed to enable the exchanging of information between ATM participants. An unique identifier of this MEP has been defined: PSPULL-MEP. The PSPULL-MEP is characterized as follows: - Conversation direction: a composition of 1 way (Publisher-> Consumer) and SRR-MEP; the latter is used by the consumer to retrieve the information/message. This is the difference with respect to the PSPUSH-MEP. - Cardinality: many-many - Decoupling: Time decoupling; Space decoupling, Synchronization decoupling. The main difference with respect to the other MEPs is the support of full time, space and synchronization decoupling. For what concerns the OPULL-MEP, it is important to note that in this case the subscriber retrieves (by SRR-MEP) the messages from an intermediary and not directly from the message source as happens for OPULL-MEP. This characterization is further detailed as part of the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities, events and QoS concerning applicable to this MEP. In particular the entities concerning this MEP are Message Topic, Intermediary, Publisher, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0015
Title	Support of Topic Based Publish/Subscribe Push Message Exchange Pattern
Requirement	The SWIM-TI Messaging shall provide the Topic based Push style Publish/Subscribe Message Exchange Pattern (TPSPUSH-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEPs). Push/Pull Publish/Subscribe MEPs can be further specialized as follows: - Topic based P/S, - Type based P/S, - Content based P/S, - Channel based P/S. The Topic based Publish/Subscribe Push is one of the identified MEPs needed to enable the exchanging of information between ATM participants. An unique identifier of this MEP has been defined: TPSPUSH-MEP. This characterization is further detailed as part of the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities, events and QoS concerning applicable to this MEP. In particular the entities concerning this MEP are Message Topic, Intermediary, Publisher, Subscriber, Subscription and Subscription handler.
Category	<Functional>

Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0020
Title	Support of Topic Based Publish/Subscribe Pull Message Exchange Pattern
Requirement	The SWIM-TI Messaging shall provide the Topic Based Pull style Publish/Subscribe Message Exchange Pattern (TPSPULL-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEPs). Push/Pull Publish/Subscribe MEPs can be further specialized as follows: - Topic based P/S, - Type based P/S, - Content based P/S, - Channel based P/S. The Topic Based Publish/Subscribe Pull is one of the identified MEPs needed to enable the exchanging of information between ATM participants. An unique identifier of this MEP has been defined: TPSPULL-MEP.

	This characterization is further detailed as part of the Message Queue and Message Topic characterization defined by PJ.17-01 This characterization describes entities, events and QoS concerning applicable to this MEP. In particular the entities concerning this MEP are Message Topic, Intermediary, Publisher, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0025
Title	Subscribe for TPSPULL-MEP
Requirement	The SWIM-TI Messaging TPSPULL-MEP shall allow subscribers to subscribe to Message Topic.
Status	<validated>
Rationale	Subscription event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary, Subscriber, Subscription and Subscription handler.
Category	<Functional>

Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0030
Title	Subscribe for TPSPUSH-MEP
Requirement	The SWIM-TI Messaging TPSPUSH-MEP shall allow subscribers to subscribe to Message Topic.
Status	<validated>
Rationale	Subscription event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0035
Title	Unsubscribe for TPSPULL-MEP
Requirement	The SWIM-TI Messaging TPSPULL-MEP shall allow subscribers to unsubscribe from Message Topic.
Status	<validated>
Rationale	Unsubscription event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0040
Title	Unsubscribe for TPSPUSH-MEP
Requirement	The SWIM-TI Messaging TPSPUSH-MEP shall allow subscribers to unsubscribe from Message Topic.
Status	<validated>
Rationale	Unsubscription event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary, Subscriber, Subscription and Subscription handler.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0045
Title	Publish for TPSPUSH-MEP and TPSPULL-MEP
Requirement	The SWIM-TI Messaging TPSPUSH-MEP and TPSPULL-MEP shall provide publishers with non-blocking capability to append messages to Message Topic.
Status	<validated>
Rationale	Publication event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary and Publisher.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0050
Title	Receive messages for TPSPUSH-MEP and TPSPULL-MEP
Requirement	The SWIM-TI Messaging TPSPUSH-MEP and TPSPULL-MEP shall provide subscribers with one or more of the following capabilities allowing to receive messages: - Synchronous and blocking receive, which will block until an appropriate message is available. - Synchronous and non-blocking receive (a polling operation), which will check the

	status of the topic and return a message if available, or a not available indication otherwise. - Asynchronous notify operation, which will issue an event notification when a message is available in the associated topic.
Status	<validated>
Rationale	Message receiving event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this requirement are Message Topic, Intermediary and Subscriber.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0055
Title	Support of Fully Decoupled Request/Reply Message Exchange Pattern
Requirement	The SWIM-TI Messaging shall provide the Fully Decoupled Request/Reply Message Exchange Pattern (FDRR-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange

Company General Use

	Patterns (MEPs). The Fully Decoupled Request/Reply or Request/Response is one of the identified MEPs needed enabling the exchanging of information between ATM participants. An unique identifier of this MEP has been defined: FDRR-MEP. The FDRR-MEP is characterized as follows: - Conversation direction: 2 way (Consumer-> Provider-> Consumer) - Cardinality: 1-1 - Decoupling: Time decoupling; Space decoupling, Synchronization. This characterization is further detailed as part of the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities, events and QoS concerning applicable to this MEP. In particular the entities concerning this MEP are Message Queue, Intermediary, Sender and Receiver.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0060
Title	Support of Fully Decoupled Request/Multi-Reply Message Exchange Pattern
Requirement	The SWIM-TI Messaging shall provide the Fully Decoupled Request/Multi-Reply

	Message Exchange Pattern (FDRMR-MEP).
Status	<validated>
Rationale	Distribution function is the core function of the SWIM-TI Messaging. The Distribution function is realized via the support to specific Message Exchange Patterns (MEPs). The Fully Decoupled Request/Multi-Reply or Request/Multi-Response is one of the identified MEPs needed enabling the exchanging of information between ATM participants. This MEP is a extension of the FDRR-MEP which supports more than one response message.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0065
Title	Append for FDRR-MEP and FDRMR-MEP
Requirement	The SWIM-TI Messaging FDRR-MEP and FDRMR-MEP shall provide senders with non-blocking capability to append messages to Message Queue.
Status	<validated>
Rationale	Message append event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this

	requirement are Message Queue, Intermediary and Sender.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0070
Title	Receive for FDRR-MEP and FDRMR-MEP
Requirement	The SWIM-TI Messaging FDRR-MEP and FDRMR-MEP shall provide receivers with one or more of the following capabilities allowing to receive messages: - Synchronous and blocking receive, which will block until an appropriate message is available. - Synchronous and non-blocking receive (a polling operation), which will check the status of the queue and return a message if available, or a not available indication otherwise. - Asynchronous notify operation, which will issue an event notification when a message is available in the associated queue.
Status	<validated>
Rationale	Message receiving event/operation as detailed in the Message Queue and Message Topic characterization defined by PJ.17-01. In particular the entities concerning this

	requirement are Message Queue, Intermediary and Receiver.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0075
Title	Enable request retries in Request/Response when no response within a time period
Requirement	The SWIM-TI Messaging shall provide, in the case of Request/Response interaction, the capability to perform a predefined number of automatic request retries in case no response is received within predefined time duration.
Status	<validated>
Rationale	To handle network failures and to provide some transparency during failover; it is necessary to support automatic request retries. This requirement contributes to support ED-133 IOP-FSM-142-MDW.This requirement covers NIST security controls SI-4 a.1
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>

Point of View	<SWIM-TI provider>
Roles	<Requestor><Responder>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0080
Title	Messaging level publisher and consumer entities unique identification
Requirement	The SWIM-TI Messaging shall provide mechanisms to uniquely identify publisher and consumer entities.
Status	<validated>
Rationale	Application using the Messaging can be reached regardless of how they are connected. It is a sort of data enrichment used for addressing purpose. It is referring to SWIM-TI layer addresses. This requirement covers NIST security control IA-9.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publisher><Publication consumer><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0010.0085
Title	Messaging level sender and receiver entities unique identification
Requirement	The SWIM-TI Messaging shall provide mechanisms to uniquely identify sender and receiver entities.
Status	<validated>
Rationale	Application using the Messaging can be reached regardless of how they are connected. It is a sort of data enrichment used for addressing purpose. It is referring to SWIM-TI layer addresses. This requirement covers NIST security control IA-9.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Requestor><Responder>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0005
Title	Message level lifespan/lifetime Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of message with non-zero/specified lifespan message level lifespan/lifetime Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message level lifespan/expiration QoS is defined as follows: + This characteristic indicates if and when the message will expire. - Message lifespan is zero/unspecified for messages which do not expire. - Message lifespan is non-zero/specified for messages which do expire. + Message expiry time can be expressed in relative and/or absolute time. - Relative expiry time represents the duration for which the message is to be considered not expired. The actual expiry time could be computed based on the time when the message is sent or created or received (by consumer or intermediary). - Absolute expiry time represents the absolute time when the message will expire. In order to avoid message starvation in MQ and MT (resources saving) messages which will not expire are not allowed. This design decision is also coherent with the fact that advisory information (AI/MET) have typically a limited lifetime. Expired messages will be routed to a pre-configured “Dead Letter Queue” (context-based filtering and routing).
Category	<Functional>
Profile Part	<PP Core>

Company General Use

Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0010
Title	Message Queue level lifespan/lifetime Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of Non-Temporary Queue Message Queue level lifespan/lifetime Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Queue level lifespan/lifetime Quality of Service is defined as follows: + This characteristic indicates if the message queue survives disconnection of interacting entities. - A Temporary Message Queue is a message queue which is deleted when interacting entities disconnect from it (message sending/receiving is either terminated properly by sender/receiver before it disconnects or interrupted abruptly due to unexpected disconnection of sender/receiver). - Non-Temporary Queue is a message queue which survives disconnection of the interacting entities. Currently there are no needs to allow temporary queue. Furthermore, temporary

	queues may be also considered a possible security vulnerability. Finally, creation of messaging resources must be strictly controlled by the administrator of the intermediary to prevent exhausting its resources.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0015
Title	Message Topic level lifespan/lifetime Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of Non-Temporary Topic Message Topic level lifespan/lifetime Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Topic level lifespan/lifetime Quality of Service is defined as follows: + This characteristic indicates if the message topic survives disconnection of interacting entities. - A Temporary Message Topic is a message topic which is deleted when interacting entities disconnect from it (message sending/receiving is either terminated properly

	by publisher/subscriber before it disconnects or interrupted abruptly due to unexpected disconnection of publisher/subscriber). - Non-Temporary Topic is a message topic which survives disconnection of the interacting entities. Currently there are no needs to allow temporary topic. Furthermore, temporary topic may be also considered a possible security vulnerability. Finally, creation of messaging resources must be strictly controlled by the administrator of the intermediary to prevent exhausting its resources.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0020
Title	Subscription level lifespan/lifetime Quality of Service - subscription with zero/unspecified lifespan
Requirement	The SWIM-TI Messaging shall provide the support of subscription with zero/unspecified lifespan subscription level lifespan/lifetime Quality of Service.
Status	<validated>

Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Subscription level lifespan/lifetime Quality of Service is defined as follows: + This characteristic indicates if and when the subscription will expire. - Subscription lifespan is zero/unspecified for subscription which do not expire. The subscription is cancelled when unsubscription request is submitted and accepted. - Subscription lifespan is non-zero/specified for subscription which do expire. Subscription expiration has the same effect of the unsubscription ("cancelled" status). + Subscription expiry time can be expressed in relative and/or absolute time. - Relative expiry time represents the duration for which the subscription is to be considered not expired. The actual expiry time could be computed based on the time when the subscription is accepted. - Absolute expiry time represents the absolute time when the subscription will expire.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0021

Title	Subscription level lifespan/lifetime Quality of Service - subscription with non-zero/specified lifespan
Requirement	The SWIM-TI Messaging shall provide the support of subscription with non-zero/specified lifespan subscription level lifespan/lifetime Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01.This characterization describes entities and applicable QoS. Subscription level lifespan/lifetime Quality of Service is defined as follows: + This characteristic indicates if and when the subscription will expire. - Subscription lifespan is zero/unspecified for subscription which do not expire. The subscription is cancelled when unsubscription request is submitted and accepted. - Subscription lifespan is non-zero/specified for subscription which do expire. Subscription expiration has the same effect of the unsubscription ("cancelled" status). + Subscription expiry time can be expressed in relative and/or absolute time. - Relative expiry time represents the duration for which the subscription is to be considered not expired. The actual expiry time could be computed based on the time when the subscription is accepted. - Absolute expiry time represents the absolute time when the subscription will expire.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0025
Title	Message level priority ordering guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of message level priority ordering guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message level priority ordering guarantees Quality of Service is defined as follows: + This characteristic indicates the relative message priority: - Message priority is a non-negative integer. Higher numbers denote higher priority. At service level it is possible to indicate that messages have different priorities (end to end).To guarantee that this needs is covered end to end it is needed to select the Message Priority based ordering for Message Queue or Message Topic. It makes no sense to use message priority and to select FIFO ordering for Message Queue or Message Topic. At service level it is also possible to indicate that messages have no priority (default priority). In this case it makes no sense to select the Message Priority based ordering for Message Queue or Message Topic. The FIFO ordering should be used.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0030
Title	FIFO Message Queue level priority ordering guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of FIFO message queue level ordering guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Queue level ordering guarantees Quality of Service is defined as follows: + This characteristic indicates the Message Queue ordering strategy: - FIFO (First In First Out, message priorities are ignored), - Message Priority (higher priority messages are dequeued first, messages with the same priority are handled by applying the FIFO strategy), + The Message Priority Message Queue Ordering strategy can require: - strict ordering: Intermediaries MUST handle the messages according to their priority. - best effort ordering: Intermediaries SHOULD do their best to handle the messages according to their priority. At service level it is possible to indicate that Message Queue FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. At service level it is also possible to indicate that Message Priority based Message Queue ordering is needed. This QoS makes sense only if Message level priority QoS is required. Currently the strict message priority based ordering is not supported.
Category	<Functional>
Profile Part	<PP Core>

Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0031
Title	Best effort message priority Message Queue level priority ordering guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of best effort message priority message queue level ordering guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Queue level ordering guarantees Quality of Service is defined as follows: + This characteristic indicates the Message Queue ordering strategy: - FIFO (First In First Out, message priorities are ignored), - Message Priority (higher priority messages are dequeued first, messages with the same priority are handled by applying the FIFO strategy), + The Message Priority Message Queue Ordering strategy can require: - strict ordering: Intermediaries MUST handle the messages according to their priority. - best effort ordering: Intermediaries SHOULD do their best to handle the messages

	according to their priority. At service level it is possible to indicate that Message Queue FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. At service level it is also possible to indicate that Message Priority based Message Queue ordering is needed. This QoS makes sense only if Message level priority QoS is required. Currently the strict message priority based ordering is not supported.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0035
Title	FIFO Message Topic level priority ordering guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of FIFO message topic level ordering guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization

	defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Topic level ordering guarantees Quality of Service is defined as follows: + This characteristic indicates the Message Topic ordering strategy: - FIFO (First In First Out, message priorities are ignored), - Message Priority (higher priority messages are delivered first, messages with the same priority are handled by applying the FIFO strategy), + The Message Priority Message Topic Ordering strategy can require: - strict ordering: Intermediaries MUST handle the messages according to their priority. - best effort ordering: Intermediaries SHOULD do their best to handle the messages according to their priority. At service level it is possible to indicate that Message Topic FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. At service level it is also possible to indicate that Message Priority based Message Topic ordering is needed. This QoS makes sense only if Message level priority QoS is required. Currently the strict message priority based ordering is not supported.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0036
Title	Best effort message priority Message Topic level priority ordering guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of best effort message priority message topic level ordering guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Topic level ordering guarantees Quality of Service is defined as follows: + This characteristic indicates the Message Topic ordering strategy: - FIFO (First In First Out, message priorities are ignored), - Message Priority (higher priority messages are delivered first, messages with the same priority are handled by applying the FIFO strategy), + The Message Priority Message Topic Ordering strategy can require: - strict ordering: Intermediaries MUST handle the messages according to their priority. - best effort ordering: Intermediaries SHOULD do their best to handle the messages according to their priority. At service level it is possible to indicate that Message Topic FIFO ordering is needed. This QoS makes sense only if Message level priority QoS is not required. At service level it is also possible to indicate that Message Priority based Message Topic ordering is needed. This QoS makes sense only if Message level priority QoS is required. Currently the strict message priority based ordering is not supported.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0040
Title	Message level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of message level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message level durability QoS is defined as follows: + This characteristic indicates if the message can be lost while in transit due intermediary failure and/or restart: - Intermediaries do not take extra care to ensure that Non-Durable messages are not lost while in transit. - Intermediaries do take care (e.g. store to stable storage) that Durable messages are not lost while in transit. At service level it is possible to indicate that durable messages are needed (end to end).This QoS has to be properly combined with durability configured for the other entities in order to guarantee the end to end needs. For instance there are no guarantees for durable messages sent to non-durable MQ. This is the recommended message durability QoS. At service level it is also possible to indicate that durable messages are not needed (end to end). In this case it makes no sense to select the Durable Message Queue or Message Topic QoS.

Company General Use

	Volatile or non-durable MQ/MT should be used.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0045
Title	Message Queue level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of message queue level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Queue level durability QoS is defined as follows: + This characteristic indicates if the message queue and the messages it holds can be lost due intermediary failure and/or restart: - A Non-Durable Message Queue is a Non-Temporary Message Queue which might not survive a failure/restart of the intermediary. A Temporary Message Queue is by definition a Non-Durable Message Queue (no obligations on the intermediary).

	- A Volatile Message Queue is a Non-Temporary Message Queue which must survive a failure/restart of the intermediary. A Volatile Message Queue might be purged if/when the intermediary fails and/or restarts irrespective of the durability of the messages it holds. - A Durable Message Queue is a Non-Temporary Message Queue which must survive a failure/restart of the intermediary preserving at least all Durable messages it holds. At service level it is possible to indicate that Message Queue Non-Durable durability is needed. This QoS makes sense only if at non-durable messages QoS is required at message level. At service level it is also possible to indicate that Message Queue Volatile durability is needed. This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). Finally, at service level it is possible to indicate that Message Queue Durable durability is needed. This is the recommended MQ durability QoS.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0050
Title	Message Topic level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of message topic level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Message Topic level durability QoS is defined as follows: + This characteristic indicates if the message topic, the messages it holds and subscriptions can be lost due intermediary failure and/or restart: - A Non-Durable Message Topic is a Non-Temporary Message Topic which might not survive a failure/restart of the intermediary. A Temporary Message Topic is by definition a Non-Durable Message Topic (no obligations on the intermediary). - A Volatile Message Topic is a Non-Temporary Message Topic which must survive a failure/restart of the intermediary. A Volatile Message Topic might be purged if/when the intermediary fails and/or restarts irrespective of the durability of the messages it holds. - A Durable Message Topic is a Non-Temporary Message Topic which must survive a failure/restart of the intermediary preserving at least all Durable messages it holds. At service level it is possible to indicate that Message Topic Non-Durable durability is needed. This QoS makes sense only if at non-durable messages QoS is required at message level. At service level it is also possible to indicate that Message Topic Volatile durability is needed. This QoS does not guarantees that messages are not lost irrespective of the message level durability QoS (durable or non-durable messages). Finally, at service level it is possible to indicate that Message Topic Durable durability is needed. This is the recommended MT durability QoS.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0055
Title	Subscription level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of Subscription level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Subscription level durability QoS is defined as follows: + This characteristic indicates if the intermediary has to accumulate messages matching the subscription irrespective of the presence of actively connected subscriber: - In case of Non-Durable Subscription only the subscribers that are actively connected to the Message Topic receive messages matching the subscription. - In case of Durable Subscription the messages matching the subscription must be accumulated until deleted or expired while the subscriber is not actively connected. When the subscriber becomes actively connected, it can receive messages published while it was not connected. Durable Subscriptions applies only to Non-Temporary Topics. In general, service level requirements may or may not constrain this QoS. It could be possible to allow both durable and non-durable subscriptions demanding to the specific subscribers to select the right durability. At service level it is possible to indicate that non-durable subscription QoS is needed.

	However, taking into account that aircraft PP SWIM Node are not always connected to the ground PP SWIM Node, this QoS is not allowed for aircraft subscriptions. At service level it is also possible to indicate that durable subscription QoS is needed. Taking into account that aircraft PP SWIM Node are not always connected to the ground PP SWIM Node, this QoS is mandatory for aircraft subscriptions. Ground applications subscribing to aircraft provided services may decide to use durable or non-durable subscriptions (assuming the service design will not constrain this QoS). However, this is the recommended Subscription durability QoS also for ground subscriptions.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0060
Title	Volatile Subscription handler level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of volatile subscription handler level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization

	defined by PJ.17-01. This characterization describes entities and applicable QoS. Subscription handler level durability QoS is defined as follows: + This characteristic indicates if the Subscription handler and the subscriptions it holds can be lost due intermediary failure and/or restart: - A Non-Durable Subscription handler might not survive a failure/restart of the intermediary. - A Volatile Subscription handler must survive a failure/restart of the intermediary. It might be purged if/when the intermediary fails and/or restarts irrespective of the durability of the subscriptions it holds. - A Durable Subscription handler must survive a failure/restart of the intermediary preserving at least all Durable subscriptions it holds. Non-Durable durability is not allowed. At service level it is possible to indicate that Subscription handler Volatile durability is needed. This QoS does not guarantees that subscriptions are not lost irrespective of the subscription level durability QoS (durable or non-durable).
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0061
Title	Durable Subscription handler level durability Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of durable subscription handler level durability Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Subscription handler level durability QoS is defined as follows: + This characteristic indicates if the Subscription handler and the subscriptions it holds can be lost due intermediary failure and/or restart: - A Non-Durable Subscription handler might not survive a failure/restart of the intermediary. - A Volatile Subscription handler must survive a failure/restart of the intermediary. It might be purged if/when the intermediary fails and/or restarts irrespective of the durability of the subscriptions it holds. - A Durable Subscription handler must survive a failure/restart of the intermediary preserving at least all Durable subscriptions it holds. At service level it is possible to indicate that Subscription handler Durable durability is needed. This is the recommended Subscription handler durability QoS.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0065
Title	Point-to-point At-Most-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of point-to-point At-Most-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01.This characterization describes entities and applicable QoS. Point-to-point At-Most-Once delivery guarantees Quality of Service is defined as follows: - Message passing between two directly connected entities is said to have At-Most-Once delivery guarantee, if it is ensured that the message cannot be delivered multiple times, even if a network error occurs. Depending on the service level NFRs, it is possible to indicate that the At-Most-Once Point-to-point delivery guarantees QoS is needed.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0070
Title	Point-to-point At-Least-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of point-to-point At-Least-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01.This characterization describes entities and applicable QoS. Point-to-point At-Least-Once delivery guarantees Quality of Service is defined as follows: - Message passing between two directly connected entities is said to have At-Least-Once delivery guarantee, if it is ensured that the message cannot be lost, even if a network error occurs. Depending on the service level NFRs, it is possible to indicate that the At-Least-Once point-to-point delivery guarantees QoS is needed.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0071
Title	Point-to-point Exactly-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of point-to-point Exactly-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Point-to-point Exactly-Once delivery guarantees Quality of Service is defined as follows: - Message passing between two directly connected entities is said to have Exactly-Once delivery guarantee, if it has both "At-Most-Once" and "At-Least-Once" delivery guarantees. Exactly-Once delivery guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability. Depending on the service level NFRs, it is possible to indicate that the Exactly-Once point-to-point delivery guarantees QoS is needed.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0075
Title	Point-to-point No delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of point-to-point No delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. Point-to-point No delivery guarantees Quality of Service is defined as follows: - Message passing between two directly connected entities is said to have No delivery guarantees, if it has neither "At-Most-Once" nor "At-Least-Once" delivery guarantees. Depending on the service level NFRs, it is possible to indicate that no point-to-point delivery guarantees are needed. This connection level delivery guarantees QoS is not applicable to air-ground connections.
Category	<Functional>
Profile Part	<PP Ground>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0080
Title	End-to-end At-Most-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of end-to-end At-Most-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. End-to-end At-Most-Once delivery guarantees Quality of Service is defined as follows: - End to end messaging is said to have At-Most-Once delivery guarantee, if it is ensured that the message cannot be delivered multiple times, even if network and/or intermediary failures/restarts occur. Depending on the service level NFRs, it is possible to indicate that the At-Most-Once end to end delivery guarantees QoS is needed. This is an end to end QoS constraining the point-to-point delivery guarantees and durability QoSs.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0085
Title	End-to-end At-Least-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of end-to-end At-Least-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. End-to-end At-Least-Once delivery guarantees Quality of Service is defined as follows: - End to end messaging is said to have At-Least-Once delivery guarantee, if it is ensured that the message cannot be lost, even if network and/or intermediary failures/restarts occur. Depending on the service level NFRs, it is possible to indicate that the At-Least-Once Connection level delivery guarantees QoS is needed. This is an end to end QoS constraining the point-to-point delivery guarantees and durability QoSs.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0086
Title	End-to-end Exactly-Once delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of end-to-end Exactly-Once delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01.This characterization describes entities and applicable QoS. End-to-end Exactly-Once delivery guarantees Quality of Service is defined as follows: - End to end messaging is said to have Exactly-Once delivery guarantee, if it has both "At-Most-Once" and "At-Least-Once" delivery guarantees. Exactly-Once delivery guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability. Depending on the service level NFRs, it is possible to indicate that the Exactly-Once end to end delivery guarantees QoS is needed. This is an end to end QoS constraining the point-to-point delivery guarantees and durability QoSs.
Category	<Functional>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0090
Title	End-to-end No delivery guarantees Quality of Service
Requirement	The SWIM-TI Messaging shall provide the support of end-to-end No delivery guarantees Quality of Service.
Status	<validated>
Rationale	This requirement is based on the Message Queue and Message Topic characterization defined by PJ.17-01. This characterization describes entities and applicable QoS. End-to-end No delivery guarantees Quality of Service is defined as follows: - End to end messaging is said to have No delivery guarantee, if it has neither "At-Most-Once" nor "At-Least-Once" delivery guarantees. Depending on the service level NFRs, it is possible to indicate that no end to end delivery guarantees are needed. In this case there are no constraints on the connection level and durability QoS used.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0105
Title	SWIM-TI Messaging support of messages and other traffic prioritization
Requirement	The SWIM-TI Messaging shall enable prioritization between messages and prioritization between messages and other traffic distributed on the same underlying communication network.
Status	<validated>
Rationale	To support various types of services over the same communication network. Although the concrete implementation is internal to the SWIM Node, some guidance/suggestions have been identified. The implemented solution should be based on composition of class Of services at SWIM Node level and class of services at network level. Assigning a CoS to a SWIM service consists in assigning that CoS to concerned messaging resources (e.g. message queue). Two or more CoSs at SWIM Node level may be assigned to the same CoS at network level (this is configurable). In this case the prioritization between the two SWIM Node level CoSs is enforced at SWIM Node level.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

4.3.1.1.2 Message routing

[REQ]

Identifier	REQ-17.01-TS-0020.0005
Title	Subject based routing
Requirement	The SWIM-TI Message Routing shall provide message level subject-based routing relying on message properties.
Status	<validated>
Rationale	The SWIM-TI Message Routing shall determine the destination of a message. The subject-based routing supported by the profile relies on message properties/metadata added by the producer and handled by the intermediary messaging infrastructure. Message properties/metadata include (but are not limited to) target destination, message priority, service to which the message concerns to, etc.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0010
Title	Context-based routing
Requirement	The SWIM-TI Message Routing shall provide message level context-based routing.
Status	<validated>
Rationale	Context-based routing is used to handle the non-nominal case/failure transparency through, for instance, retries and sending the message to alternative destinations.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0015
Title	Message expiration Context-based routing
Requirement	The SWIM-TI Message Routing shall provide message expiration context-based

	routing.
Status	<validated>
Rationale	Message expiration is an event that has to be properly handled by the SWIM-TI. It is up to routing policy to indicate: a) if the expired message has to be just dropped or moved to a dedicated queue (for monitoring purposes); b) event to be logged and c) how long the message will be kept in the queue (in case the message is routed to a specific queue).
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0020
Title	Undelivered message Context-based routing
Requirement	The SWIM-TI Message Routing shall provide undelivered message context-based routing.
Status	<validated>
Rationale	A message, which is not expired yet, could be discarded because it cannot be delivered (e.g. maximum number of retries). It is up to routing policy to indicate: a) if the message has to be just dropped or moved to a dedicated queue (for monitoring

	purposes); b) event to be logged and c) how long the message will be kept in the queue (in case the message is routed to a specific queue).
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0025
Title	Message dropped Context-based routing
Requirement	The SWIM-TI Message Routing shall provide message dropped context-based routing.
Status	<validated>
Rationale	A message from a sender/publisher could be dropped (e.g. maximum size, message rate). It is up to routing policy to indicate: a) if the message has to be just discarded or moved to a dedicated queue (for monitoring purposes); b) event to be logged and c) how long the message will be kept in the queue (in case the message is routed to a specific queue).
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>

Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0045
Title	Aircraft data domain segregation and default context-based message routing
Requirement	The default context-based routing policy for dropped, undelivered and expired incoming and outgoing messages shall be to permanently drop the message.
Status	<validated>
Rationale	Routing to avionics system must be done accordingly to the aircraft type design configuration, and with respect to data domain segregations. Undeliverable message are always dropped without notice in avionics functions.
Category	<Functional>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Routing Purple Profile

4.3.1.1.3 Message-filtering

[REQ]

Identifier	REQ-17.01-TS-0030.0005
Title	Subject based filtering
Requirement	The SWIM-TI Message Filtering shall provide subject-based filtering relying on message properties.
Status	<validated>
Rationale	The SWIM-TI Message Filtering shall determine if the message has to be filtered out. The subject-based filtering supported by the profile relies on message properties/metadata added by the producer and handled by the intermediary messaging infrastructure.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publisher><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0010
Title	Context-based filtering
Requirement	The SWIM-TI Message Filtering shall provide context-based filtering
Status	<validated>
Rationale	The SWIM-TI Message Filtering shall determine if the message has to be filtered out. Context-based filtering is used to handle the non-nominal case/failure through filtering out messages according to specific context-based filtering criteria.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publisher><Publication consumer><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0015
Title	Message expiration Context-based filtering
Requirement	The SWIM-TI Message Filtering shall provide message expiration context-based filtering.
Status	<validated>
Rationale	Expired messages are filtered-out and then handled by context-based message routing according to the applicable policy.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0020
Title	Undelivered message Context-based filtering
Requirement	The SWIM-TI Message Filtering shall provide undelivered message context-based filtering.
Status	<validated>
Rationale	Undelivered messages are filtered-out and then handled by context-based message

	routing according to the applicable policy.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0025
Title	Message dropped Context-based filtering
Requirement	The SWIM-TI Message Filtering shall provide message dropped context-based filtering.
Status	<validated>
Rationale	Dropped messages are filtered-out and then handled by context-based message routing according to the applicable policy.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0030
Title	Subject based Filtering Criteria at subscription time
Requirement	The SWIM-TI Message Filtering shall allow subscribers to provide subject based filtering criteria at subscription time.
Status	<validated>
Rationale	This requirement guarantees that in one operation (subscription time) the subscribers are able to subscribe to such topic and also to set specific filtering criteria. Following the acceptance of the subscription the subject-based filtering criteria cannot be removed/updated. In order to remove/update the active filtering criteria it is needed to unsubscribe and subscribe again with no/updated filtering criteria. Subject based filtering criteria provided at subscription time (if any) are evaluated in AND relationship with subject based filtering criteria available in the Filtering policy.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscription handler><Subscriber>
Selfstanding set	<Not applicable>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0050
Title	Message Topic side Subject based filtering enforcement
Requirement	Subject-based filtering shall be enforced on the Message Topic side.
Status	<validated>
Rationale	The SWIM-TI Message Filtering shall determine if the message has to be filtered out. The subject-based filtering is always enforced on the Message Topic side and never on the Publisher or Subscriber side.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0055
Title	Aircraft data domains segregation and message filtering
Requirement	Messages filtered out following message filtering policies enforcement shall be marked as drop.
Status	<validated>
Rationale	Aircraft domain reference model is specified in ARINC Report 664 P5 Aircraft Data Network which provides a notional model of the aircraft networking among four domains. Filtering and routing to avionics system must be done accordingly to the aircraft type design configuration, and with respect to data domain segregations. Undeliverable message are always dropped without notice in avionics functions.
Category	<Functional>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0060
Title	Aircraft data domains segregation and message filtering policy definition
Requirement	Subject, context and content based SWIM message filtering policies definitions shall contain the required information to filter-out messages not associated to known AISD avionics functions as per air transport operator procedures.
Status	<validated>
Rationale	Aircraft domain reference model is specified in ARINC Report 664 P5 Aircraft Data Network which provides a notional model of the aircraft networking among four domains. Filtering messages to avionics systems must be done with respect to data domain segregations
Category	<Functional>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

4.3.1.1.4 Message enrichment

[REQ]

Identifier	REQ-17.01-TS-0050.0015
Title	SWIM-TI Messaging support of message enrichment
Requirement	The SWIM-TI Messaging shall provide Message enrichment mechanisms.
Status	<validated>
Rationale	Message enrichment mechanisms allow the enrichment of information distributed via messaging protocol used at SWIM-TI layer (internal to SWIM-TI and at the perimeter between the ATM layer and SWIM-TI layer) by adding application and/or infrastructure specific metadata.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Enrichment Purple Profile

4.3.1.1.5 Messaging Policy management

[REQ]

Identifier	REQ-17.01-TS-0020.0030
Title	Policy Based SWIM-TI Message Routing
Requirement	The SWIM-TI Message Routing shall allow routing by enforcing Routing Policy.
Status	<validated>

Rationale	Not all the information exchanged through the SWIM-TI may need the same handling by the SWIM-TI Message Routing. The specific routing paths are defined in a Routing policy which is enforced to properly route the message. This is applicable to both subject-based and context-based routing. In particular the routing policy indicates if and how to handle events concerning context-based routing. For expired, dropped and undelivered messages, the policy indicates: a) if the message has to be routed to a dedicated queue (for monitoring purposes) or not ; b) event to be logged and c) how long the message will be kept in the queue (in case the message is routed to a specific queue).
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0035
Title	Static definition of the Routing policy
Requirement	The SWIM-TI Message Routing shall allow to statically define routing paths in the Routing Policy.
Status	<validated>
Rationale	The service specific or generic routing paths are defined in a Routing policy which is enforced to properly route the message. This is applicable to both subject-based and

	context-based routing. Routing policy can be defined statically at configuration time.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0020.0040
Title	Dynamic definition and update of the Routing policy
Requirement	The SWIM-TI Message Routing shall allow to dynamically define and update routing paths in the Routing Policy.
Status	<validated>
Rationale	The service specific or generic routing paths are defined in a Routing policy which is enforced to properly route the message. This is applicable to both subject-based and context-based routing. Routing policy can be defined and updated dynamically at run-time.
Category	<Functional>
Profile Part	<PP Ground>

Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0035
Title	Policy Based SWIM-TI Message Filtering
Requirement	The SWIM-TI Message Filtering shall allow filtering by enforcing Filtering Policy.
Status	<validated>
Rationale	The SWIM-TI Message Filtering shall determine if the message has to be filtered out. The specific filtering criteria are defined in a Filtering policy which is enforced to properly filter out the message. This is applicable to both subject-based and context-based filtering. Subject based filtering has to be implemented in accordance with Purple Profile: - filtering provided at subscription time (PS MEP). - filtering at link level (both PS and RR MEPs) - Filtering policy -> defined in subscription policy. All the above evaluated in AND condition.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>

Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0040
Title	Static definition of the Filtering policy
Requirement	The SWIM-TI Message Filtering shall allow to statically define both subject-based and context-based filtering criteria in the Filtering Policy.
Status	<validated>
Rationale	The service specific or generic filtering criteria are defined in a Filtering policy which is enforced to properly filter out the message. This is applicable to both subject-based and context-based filtering. Filtering policy can be defined statically at configuration time. Subject based filtering criteria provided at subscription time (if any) are evaluated in AND relationship with statically defined subject based filtering criteria. Subject based filtering has to be implemented in accordance with Purple Profile: - filtering provided at subscription time (PS MEP). - filtering at link level (both PS and RR MEPs) - Filtering policy -> defined in subscription policy. All the above evaluated in AND condition.
Category	<Functional>

Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0045
Title	Dynamic definition and update of the Filtering policy
Requirement	The SWIM-TI Message Filtering shall allow to dynamically define and update both subject-based and context-based filtering criteria in the Filtering Policy.
Status	<validated>
Rationale	The service specific or generic filtering criteria are defined in a Filtering policy which is enforced to properly filter out the message. This is applicable to both subject-based and context-based filtering. Filtering policy can be defined and updated dynamically at run-time. Subject based filtering criteria provided at subscription time (if any) are evaluated in AND relationship with subject based filtering criteria available in the Filtering policy. Subject based filtering has to be implemented in accordance with Purple Profile: - filtering provided at subscription time (PS MEP). - filtering at link level (both PS and RR MEPs) - Filtering policy -> defined in subscription policy.

	All the above evaluated in AND condition.
Category	<Functional>
Profile Part	<PP Ground>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0030.0046
Title	Filtering policy and filtering criteria provided by receivers and subscribers
Requirement	Any filtering criteria provided at run-time by receivers or subscribers shall be evaluated in AND relationship with applicable (if any) filtering policy,
Status	<validated>
Rationale	This requirement allows to proper combine filtering policies and filtering criteria provided by receivers/subscribers at run-time. Subject based filtering has to be implemented in accordance with Purple Profile: - filtering provided at subscription time (PS MEP). - filtering at link level (both PS and RR MEPs) - Filtering policy -> defined in subscription policy. All the above evaluated in AND condition.
Category	<Functional>

Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0095
Title	Policy Based SWIM-TI Message Quality of Service
Requirement	The SWIM-TI Messaging shall allow QoS enforcement based on Quality of Service Policy.
Status	<validated>
Rationale	The SWIM-TI Messaging is used to enable the exchanging of different types of data with different QoS requirements. The specific QoSs are defined in a QoS policy which is properly enforced in order to guarantee the configured QoS levels. Currently, the following QoS policies have been defined: Delivery guarantees, Lifetime, Durability, Ordering guarantees and CoSs.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0040.0100
Title	Static definition of Quality of Service Policy
Requirement	The SWIM-TI Messaging shall allow to statically define QoSs in the Quality of Service Policy.
Status	<validated>
Rationale	The service specific or generic QoS are defined in Quality of Service Policies which are properly enforced in order to guarantee the configured QoS levels. Quality of Service Policies are defined statically at configuration time. Currently, the following QoS policies have been defined: Delivery guarantees, Lifetime, Durability, Ordering guarantees and CoSs.
Category	<Functional>
Profile Part	<PP Core>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0050.0025
Title	Support of Policy based Compression Configurability
Requirement	The SWIM-TI Messaging shall allow to configure data compression on a Compression Policy basis.
Status	<validated>
Rationale	The SWIM-TI Messaging is used to enable the exchanging of different types of data with different compression needs and techniques. The specific configuration is defined in a Compression policy which is properly enforced.
Category	<Functional>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<Function/Behaviour><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0050.0030
Title	Static definition of Compression Policy
Requirement	SWIM-TI Messaging shall allow to statically configure the compression mechanisms in the Compression Policy.
Status	<validated>
Rationale	The service specific or generic compression mechanisms are defined in Compression Policies. Compression Policies are defined statically at configuration time.
Category	<Functional>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<Function/Behaviour><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

4.3.1.1.6 Crosscutting

[REQ]

Identifier	REQ-17.01-TS-0050.0020
Title	Support of Data Compression Techniques
Requirement	The SWIM-TI Messaging shall allow data compression.
Status	<validated>
Rationale	The SWIM-TI Messaging is used to enable data exchanges among geographically distributed entities (wide area deployment).Taking into account this deployment view, performance bottlenecks due to sizing aspects (e.g. number of entities, exchange rate, data size, etc.) could impact the overall messaging performance thus it is required to allow data compression techniques. Data compression can be realized in more than 1 one way and at distinct levels. For example, the ATM application layer can provide a compressed payload to the SWIM-TI. The SWIM-TI itself can also provide data compression. The SWIM-TI shall not prevent the use of data compression inside the SWIM-TI nor compression performed at the ATM application layer. When compression is composed with encryption cryptography techniques the following is recommended: - compression internal to SWIM-TI: not applicable because inefficient compression rate. - compression at the perimeter between ATM and SWIM-TI layers: in case encryption is used it is recommended to first compress and then to encrypt. This allows a more efficient compression.
Category	<Functional><Performance>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<Function/Behaviour><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0005
Title	Statistic Metrics provided for Publish-Subscribe pattern.
Requirement	The SWIM-TI Messaging shall provide the following metrics for the Publish/Subscribe pattern: + Number of data publications. + Time of the last data publication. + Number of failed data publications. + Number of received data publications. + Time of the last received data publication. + Number of missing data publications.
Status	<validated>
Rationale	The SWIM-TI Messaging supports several MEPs (Message Exchange Patterns) including Publish-Subscribe. It represents one of the most important capabilities and, in order to support monitoring activities, it is needed that it supports the reporting of such metrics. This requirement covers NIST security controls SI-4 a.1
Category	<Functional><Security>
Profile Part	<PP Ground>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0010
Title	Statistic Metrics provided for the Request-Response pattern
Requirement	The SWIM-TI Messaging shall provide the following metrics for the Request/Response pattern: + Number of Requests. + Time of the Last Request. + Number of Failed Requests. + Number of Successful Requests. + Maximum Response Time. + Last Response Time.
Status	<validated>
Rationale	The SWIM-TI Messaging supports several MEPs (Message Exchange Patterns) including Request-Response. It represents one of the most important capabilities and, in order to support monitoring activities, it is needed that it supports the reporting of such metrics. This requirement covers NIST security controls SI-4 a.1
Category	<Functional><Security>
Profile Part	<PP Ground>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0015
Title	Logging of events related to Messaging policies
Requirement	The SWIM-TI Messaging should log with configurable levels of severity and verbosity events related to the enforcement of: - Routing policies, - Filtering policies, - Quality of Service policies.
Status	<validated>
Rationale	When one or more types of messaging policy are in place, logging of relevant events is useful for monitoring purposes. Different levels of severity and verbosity could be configured for all the services or on a service basis. Notice that logging of events concerning security functions (e.g. certificate validation) is not covered by this requirement. These security related logging is part of functional and non-functional security requirements. This requirement covers NIST security controls SI-4 a.1.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0016
Title	Logging of events related to advanced Messaging policies
Requirement	The SWIM-TI Messaging should log with configurable levels of severity and verbosity events related to the enforcement of Compression policies.
Status	<validated>
Rationale	This requirement complements REQ-17.01-TS-0070.0015 with advanced messaging policies.
Category	<Functional><Security>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0017

Title	Messaging policies management via administrative interfaces
Requirement	Messaging policies shall be defined, updated, enabled and disabled via administrative interfaces.
Status	<validated>
Rationale	Only administrators are authorized to manage messaging policies.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0070.0018
Title	Messaging resources management via administrative interfaces
Requirement	Message Queues, Message Topics and Subscription handlers lifecycle and configuration management shall be via administrative interfaces.
Status	<validated>
Rationale	Only administrators are authorized to manage messaging resources.
Category	<Functional><Interface>

Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Messaging Policy Management Purple Profile

4.3.1.2 Security

This section provided security requirements concerning the functional view. Requirements have been grouped per security function.

4.3.1.2.1 Identity Management

[REQ]

Identifier	REQ-17.01-TS-0170.0010
Title	Digital identities administrative procedures and services
Requirement	Digital identities shall be managed via Identity Management administrative procedures and services.
Status	<validated>
Rationale	Digital identities used in security functions are managed (e.g. creation, renewal, revocation, storing, validation, etc.) via Identity Management infrastructure that encompasses: - administrative procedures, - local and remote resources,

	- local and remote services. IdM procedures and services must comply with applicable regulations, security management policies and processes.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Identity Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0170.0015
Title	Cryptographic keys administrative procedures and services
Requirement	Cryptographic keys shall be managed via Identity Management administrative procedures and services.
Status	<validated>
Rationale	Cryptographic keys used in security functions are managed via Identity Management infrastructure that encompasses: - administrative procedures, - local and remote resources, - local and remote services.

	IdM procedures and services must comply with applicable regulations, security management policies and processes.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Identity Management Purple Profile

4.3.1.2.2 Authentication

[REQ]

Identifier	REQ-17.01-TS-0110.0300
Title	Senders and Message Queue mutual authentication
Requirement	The SWIM-TI authentication shall provide mutual authentication between senders and message queue.
Status	<validated>
Rationale	In the normal mode/nominal conditions the connection between senders and message queue is mutual authenticated.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0305
Title	Receiver and Message Queue mutual authentication
Requirement	The SWIM-TI authentication shall provide mutual authentication between receiver and message queue.
Status	<validated>
Rationale	In the normal mode/nominal conditions the connection between receiver and message queue is mutual authenticated.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0310
Title	Publishers and Message Topic mutual authentication
Requirement	The SWIM-TI authentication shall provide mutual authentication between publishers and message topic.
Status	<validated>
Rationale	In the normal mode/nominal conditions the connection between publishers and message topic is mutual authenticated.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0315
Title	Subscribers and Message Topic mutual authentication
Requirement	The SWIM-TI authentication shall provide mutual authentication between subscribers and message topic.
Status	<validated>
Rationale	In the normal mode/nominal conditions the connection between subscribers and message topic is mutual authenticated.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0320
Title	Subscribers and Subscription handler mutual authentication
Requirement	The SWIM-TI authentication shall provide mutual authentication between subscribers and subscription handler.
Status	<validated>

Rationale	In the normal mode/nominal conditions the connection between subscribers and subscription handler is mutual authenticated.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0325
Title	Mutual authentication and digital identity type
Requirement	The SWIM-TI authentication shall allow mutual authentication based on the same type of digital identity.
Status	<validated>
Rationale	In the normal mode/nominal conditions the mutual authentication is based on the exchanging of the same type of digital identity.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0330
Title	Mutual authentication and digital identity validation
Requirement	Two connecting entities shall validate the digital identity provided by the peer by properly combining - local digital identities validation mechanisms, and - remote digital identities validation mechanisms.
Status	<validated>
Rationale	This requirements allows to combine local (host resources) and remote (i.e. LAN, WAN) mechanisms for digital identity validation .
Category	<Functional><Security>
Profile Part	<PP Ground><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0335
Title	Digital identity validation in non-nominal conditions
Requirement	In non-nominal security conditions when remote digital identity validation mechanisms are not available, the local validation mechanisms take the precedence.
Status	<validated>
Rationale	This requirements allows to continue digital identity validation in case the remote validation mechanism are not available.
Category	<Functional><Security>
Profile Part	<PP Ground><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

4.3.1.2.3 Authorization

[REQ]

Identifier	REQ-17.01-TS-0120.0010
Title	Senders authorization
Requirement	The SWIM-TI authorization shall permit only authenticated and authorized senders to send messages to a message queue.
Status	<validated>
Rationale	Only authorized entities are allowed to access message queues. This requirement covers NIST security controls AC-3 and AC-24.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0120.0015

Title	Receiver authorization
Requirement	The SWIM-TI authorization shall permit only authenticated and authorized receiver to consume messages from a message queue.
Status	<validated>
Rationale	Only authorized entities are allowed to access message queues. This requirement covers NIST security controls AC-3 and AC-24.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0120.0020
Title	Publishers authorization
Requirement	The SWIM-TI authorization shall permit only authenticated and authorized publishers to publish messages to a message topic.
Status	<validated>
Rationale	Only authorized entities are allowed to access message topics. This requirement covers NIST security controls AC-3 and AC-24.

Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0120.0025
Title	Subscribers authorization
Requirement	The SWIM-TI authorization shall permit only authenticated and authorized subscribers to consume messages from a message topic.
Status	<validated>
Rationale	Only authorized entities are allowed to access message topics. This requirement covers NIST security controls AC-3 and AC-24.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0120.0030
Title	Subscription authorization
Requirement	The SWIM-TI authorization shall permit only authenticated and authorized subscribers to send subscription management messages to a subscription handler.
Status	<validated>
Rationale	Only authorized entities are allowed to interact with the subscription handlers.. This requirement covers NIST security controls AC-3 and AC-24.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0120.0035
Title	Authorization based on authenticated digital identity
Requirement	The SWIM-TI authorization shall use authenticated digital identity for enforcing authorization.
Status	<validated>
Rationale	Authorization enforcement is based on the authenticated digital identity. This allows authorization mechanisms to retrieve additional properties (e.g. roles) linked to that identity used for access rights check. This requirement covers NIST security controls AC-3 and AC-24.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Authorization Purple Profile

4.3.1.2.4 Confidentiality ensuring

[REQ]

Identifier	REQ-17.01-TS-0130.0010
Title	Senders-Message Queue information confidentiality
Requirement	The SWIM-TI Confidentiality ensuring shall provide information confidentiality between senders and message queue.
Status	<validated>
Rationale	Confidentiality of the Information transfer between senders and message queue has to be protected. This requirement covers NIST security control AC-17 (2), SC-8 (1) and SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0015

Title	Receiver-Message Queue information confidentiality
Requirement	The SWIM-TI Confidentiality ensuring shall provide information confidentiality between receiver and message queue.
Status	<validated>
Rationale	Confidentiality of the Information transfer between message queue and receiver has to be protected. This requirement covers NIST security control AC-17 (2), SC-8 (1) and SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0020
Title	Publishers-Message Topic information confidentiality
Requirement	The SWIM-TI Confidentiality ensuring shall provide information confidentiality between publishers and message topic.
Status	<validated>
Rationale	Confidentiality of the Information transfer between publishers and message topic has to be protected.

	This requirement covers NIST security control AC-17 (2), SC-8 (1) and SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0025
Title	Subscribers-Message Topic information confidentiality
Requirement	The SWIM-TI Confidentiality ensuring shall provide information confidentiality between subscribers and message topic.
Status	<validated>
Rationale	Confidentiality of the Information transfer between message topic and subscribers has to be protected. This requirement covers NIST security control AC-17 (2), SC-8 (1) and SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Subscriber><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0030
Title	Subscribers-Subscription handler information confidentiality
Requirement	The SWIM-TI Confidentiality ensuring shall provide information confidentiality between subscribers and subscription handler.
Status	<validated>
Rationale	Confidentiality of the Information transfer between subscribers and subscription handler has to be protected. This requirement covers NIST security control AC-17 (2), SC-8 (1) and SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0165
Title	Asymmetric Encryption Schemas for SWIM-TI Confidentiality Ensuring
Requirement	The SWIM-TI Confidentiality ensuring shall use Asymmetric encryption schema.
Status	<validated>
Rationale	Asymmetric encryption schema is widely adopted for confidentiality ensuring. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0170
Title	Symmetric Encryption Schemas for SWIM-TI Confidentiality Ensuring
Requirement	The SWIM-TI Confidentiality ensuring shall use Symmetric encryption schema.
Status	<validated>
Rationale	Symmetric encryption schema is widely adopted for confidentiality ensuring. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0175
Title	Asymmetric/Symmetric Hybrid Encryption Schemas for SWIM-TI Confidentiality Ensuring
Requirement	The SWIM-TI Confidentiality ensuring shall use Asymmetric/Symmetric Hybrid

	encryption schema.
Status	<validated>
Rationale	Asymmetric/Symmetric Hybrid encryption schema is widely adopted for confidentiality ensuring. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0035
Title	Transport level confidentiality ensuring
Requirement	The SWIM-TI Confidentiality ensuring shall rely on transport level security mechanisms.
Status	<validated>
Rationale	The SWIM-TI confidentiality ensuring is responsible for point to point information confidentiality between publishers/subscribers-message topic, subscribers-subscription handler and senders/receiver-message queue.

	This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0040
Title	Enabling end-to-end confidentiality for Message queue based information exchange
Requirement	The SWIM-TI Message distribution shall provide mechanisms to transfer message level confidentiality information between senders and receivers enabling end-to-end confidentiality without violating it.
Status	<validated>
Rationale	The SWIM-TI is not responsible for ensuring end-to-end confidentiality. It aims at enabling the transfer of security information (when needed) without violating message security attributes. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>

Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0130.0045
Title	Enabling end-to-end confidentiality for Message topic based information exchange
Requirement	The SWIM-TI Message distribution shall provide mechanisms to transfer message level confidentiality information between publishers and subscribers enabling end-to-end confidentiality without violating it.
Status	<validated>
Rationale	The SWIM-TI is not responsible for ensuring end-to-end confidentiality. It aims at enabling the transfer of security information (when needed) without violating message security attributes. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

4.3.1.2.5 Integrity and authenticity ensuring

[REQ]

Identifier	REQ-17.01-TS-0140.0010
Title	Senders-Message Queue information integrity and authenticity
Requirement	The SWIM-TI Integrity and authenticity ensuring shall provide information integrity and authenticity between senders and message queue.
Status	<validated>
Rationale	Integrity and authenticity of the Information transfer between senders and message queue has to be protected. This requirement covers NIST security controls IA-2, IA-8,IA-5 a, IA-5 b, IA-9, SC-20 a and SC-20 b.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0015
Title	Receiver-Message Queue information integrity and authenticity
Requirement	The SWIM-TI Integrity and authenticity ensuring shall provide information integrity and authenticity between receiver and message queue.
Status	<validated>
Rationale	Integrity and authenticity of the Information transfer between message queue and receiver has to be protected. This requirement covers NIST security controls IA-2, IA-8,IA-5 a, IA-5 b, IA-9, SC-20 a and SC-20 b.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0020
Title	Publishers-Message Topic information integrity and authenticity
Requirement	The SWIM-TI Integrity and authenticity ensuring shall provide information integrity and authenticity between publishers and message topic.
Status	<validated>
Rationale	Integrity and authenticity of the Information transfer between publishers and message topic has to be protected. This requirement covers NIST security controls IA-2, IA-8,IA-5 a, IA-5 b, IA-9, SC-20 a and SC-20 b.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0025
Title	Subscribers-Message Topic information integrity and authenticity
Requirement	The SWIM-TI Integrity and authenticity ensuring shall provide information integrity and authenticity between subscribers and message topic.
Status	<validated>
Rationale	Integrity and authenticity of the Information transfer between message topic and subscribers has to be protected. This requirement covers NIST security controls IA-2, IA-8,IA-5 a, IA-5 b, IA-9, SC-20 a and SC-20 b.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0030
Title	Subscribers-Subscription handler information integrity and authenticity
Requirement	The SWIM-TI Integrity and authenticity ensuring shall provide information integrity and authenticity between subscribers and subscription handler.

Status	<validated>
Rationale	Integrity and authenticity of the Information transfer between subscribers and subscription handler has to be protected. This requirement covers NIST security controls IA-2, IA-8,IA-5 a, IA-5 b, IA-9, SC-20 a and SC-20 b.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0200
Title	Asymmetric Integrity and authenticity ensuring schema
Requirement	The SWIM-TI Integrity and authenticity ensuring shall use digital signature.
Status	<validated>
Rationale	Digital signature is an asymmetric technique widely adopted to ensure integrity and authenticity. With respect to HMAC, the digital signature provides also non-repudiation. This requirement covers NIST security controls IA-2, IA-8, IA-9 and AC-4.

Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0205
Title	Symmetric Integrity and authenticity ensuring schema
Requirement	The SWIM-TI Integrity and authenticity ensuring shall use HMAC.
Status	<validated>
Rationale	HMAC (keyed-hash message authentication code) is a symmetric technique widely adopted to ensure integrity and authenticity. With respect to digital signature, HMAC does not provide non-repudiation. This requirement covers NIST security controls IA-2, IA-8, IA-9 and AC-4.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0035
Title	Transport level integrity and authenticity ensuring
Requirement	The SWIM-TI Integrity and authenticity ensuring shall rely on transport level security mechanisms.
Status	<validated>
Rationale	The SWIM-TI Integrity and authenticity ensuring is responsible for point to point information Integrity and authenticity between publishers/subscribers-message topic, subscribers-subscription handler and senders/receiver-message queue. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0040
Title	Enabling end-to-end integrity and authenticity for Message queue based information exchange
Requirement	The SWIM-TI Message distribution shall provide mechanisms to transfer message level integrity and authenticity information between senders and receivers enabling end-to-end integrity and authenticity without violating them.
Status	<validated>
Rationale	The SWIM-TI is not responsible for ensuring end-to-end integrity and authenticity. It aims at enabling the transfer of security information (when needed) without violating message security attributes. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0140.0045
Title	Enabling end-to-end integrity and authenticity for Message topic based information exchange
Requirement	The SWIM-TI Message distribution shall provide mechanisms to transfer message level integrity and authenticity information between publishers and subscribers enabling end-to-end integrity and authenticity without violating them.
Status	<validated>
Rationale	The SWIM-TI is not responsible for ensuring end-to-end integrity and authenticity. It aims at enabling the transfer of security information (when needed) without violating message security attributes. This requirement covers NIST security controls SC-8, SC-13, SC-11.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

4.3.1.2.6 Audit

[REQ]

Identifier	REQ-17.01-TS-0110.0035
Title	Policy Based Encryption and Decryption attempts auditing
Requirement	The SWIM-TI Audit shall allow to audit encryption and decryption attempts according to the specific Audit policy.
Status	<deleted>
Rationale	Encryption and decryption attempts can be audited or not according to a specific Audit policy. This requirement covers NIST security control AU-2 a. Deletion reason: no encryption/decryption at SWIM Node level.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0075
Title	Policy Based integrity and authenticity validation attempts auditing
Requirement	The SWIM-TI Audit shall allow to audit integrity and authenticity validation attempts according to the specific audit policy.
Status	<in progress>
Rationale	Integrity and authenticity attempts can be audited or not according to a specific Audit policy. This requirement covers NIST security controls AC-6 (9) and AU-2 a. At SWIM infrastructure level, the only use case for integrity and authenticity validation attempts is the message level digital signature validation for subscription management request and response messages.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0250
Title	Policy Based Authentication attempts auditing
Requirement	The SWIM-TI Audit shall allow to audit authentication attempts according to the specific audit policy.

Status	<in progress>
Rationale	Authentication attempts can be audited or not according to a specific Audit policy. This requirement covers NIST security controls AC-17 (1), AU-2 a , SI-4 g.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0251
Title	Policy Based Authorization attempts auditing
Requirement	The SWIM-TI Audit shall allow to audit authorization attempts according to the specific audit policy.
Status	<in progress>
Rationale	Authorization attempts can be audited or not according to a specific Audit policy. This requirement covers NIST security controls AC-17 (1), AU-2 a , SI-4 g.
Category	<Functional><Security>
Profile Part	<PP Core>

Domain of Interest	<Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0095
Title	Service-level specific logging
Requirement	The SWIM-TI Security shall record events with all additional data specified in the applicable service-specific Audit Policy.
Status	<in progress>
Rationale	The existence of service-specific Audit policies may supplement/override the Global (default) Audit policy. This requirement ensures that any additional data required by these Policies gets logged. This requirement covers NIST security controls AU-12 and AU-3 (1).
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0260
Title	Supporting tamper-proof information storage
Requirement	The SWIM-TI Security shall provide tamper-proof storage of sensitive information by applying encryption and digital signature.
Status	<in progress>
Rationale	Certain types of information used in aviation must be secured so as to be tamper-proof. This can include certain logs for example. Tamper-proofing means that the information will be available and uncompromised for a long period of time – at least 50 years. Tamper-proof information storage is a vital aspect of non-repudiation in aviation and is achieved applying cryptographic techniques such as digital signature. This requirement ensures coverage of NIST SP 800 53 security control SC-28.
Category	<Design><Functional><Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0265
Title	Sensitive information preservation
Requirement	The SWIM-TI Security shall allow to maintain sensitive information in an uncompromised condition for a configurable number of days to be defined either by policy or application level configuration.
Status	<in progress>
Rationale	Certain types of information used in aviation must be secured so as to be tamper-proof. This can include certain logs for example. Tamper-proofing means that the information will be available and uncompromised for a long period of time – at least 50 years. Tamper-proof information storage is a vital aspect of non-repudiation in aviation and is achieved applying cryptographic techniques such as digital signature. This requirement ensures coverage of NIST SP 800 53 security control SC-28.
Category	<Design><Functional><Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

4.3.1.2.7 Message screening

[REQ]

Identifier	REQ-17.01-TS-0150.0010
Title	Malformed messages screening
Requirement	The SWIM-TI Message screening shall allow to filter malformed messages.
Status	<validated>
Rationale	This requirement allows to protect the recipients of the message against malformed messages.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0015
Title	Malformed messages screening: message properties
Requirement	Malformed message screening shall check the validity of message properties against reference schema and assertions.
Status	<validated>
Rationale	This requirement allows to protect the recipients against messages with malformed/unknown properties. It allows also to save application level resources without processing malformed messages.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0020
Title	Malformed messages screening: message payload
Requirement	Malformed message screening shall check the syntactical validity of message payload against reference schema and assertions.
Status	<validated>
Rationale	This requirement allows to protect the recipients of the message against messages with malformed payload. It is restricted to syntactical validation. It allows also to save application level resources without processing malformed messages. Examples of validity checks include validating XML data against applicable XSDs, ASN.1 data against applicable ASN.1 modules definition, etc. Even if it is an advanced feature that could be enabled/disable per MQ/MT, in some cases it could be not possible to access the data because (e.g.) application level compression and/or encryption.
Category	<Functional><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0025

Title	Messages screening and typed message queue and topic
Requirement	The SWIM-TI Message screening shall allow to filter messages according to typed Message Queue and Topic.
Status	<validated>
Rationale	A typed message queue (or topic) is a queue for which only predefined message type(s) are allowed. This requirement allows to protect the recipients of the message against unexpected message types (irrespective of the syntactical validation of the message payload).
Category	<Functional><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0030
Title	Malicious messages screening
Requirement	The SWIM-TI Message screening shall allow to filter malicious messages.
Status	<validated>
Rationale	This requirement allows to protect the recipients of the message against malicious messages. Specific techniques are applicable depending on the message payload. For

	instance, for XML messages it is possible to detect malicious content by applying XML/XSD specific techniques. For instance, this could be implemented via safe XXE protected XML message validator.
Category	<Functional><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0035
Title	Malicious messages screening: properties and payload
Requirement	Malicious message screening shall check: - Message properties, and - Message payload.
Status	<validated>
Rationale	This requirement allows to protect the recipients of the message against malicious messages. Specific techniques are applicable depending on the message payload. For instance, for XML messages it is possible to detect malicious content by applying XML/XSD specific techniques. Both properties and payload have to be validated.

Category	<Functional><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0150.0040
Title	Message screening configurability
Requirement	Message screening shall be configurable per message queue and message topic.
Status	<validated>
Rationale	For two or more message queues/topics, different message screening needs could be required. This requirement allows to configure message screening per queue/topic.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Message Screening Purple Profile

4.3.1.2.8 Overload protection

[REQ]

Identifier	REQ-17.01-TS-0110.0245
Title	SWIM Technical Infrastructure overload protection support
Requirement	The SWIM-TI Security shall protect the overall SWIM-TI against overload resulting from: + Denial of Service Attack, or + Service Utilization above maximum levels.
Status	<in progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Taking into account the overall context and the sensitivity of the exchanged data it is required to guarantee several security properties such as (but not limited to) the information integrity, authorization and confidentiality and service (ATM-specific and Infrastructure services) consumer/provider authentication and to protect information and systems from external unknown and malicious users. This requirement assures that the SWIM Technical infrastructure is protected against overload due to attacks or to legitimate, but above thresholds, use of services; for instance number of concurrent accesses could be limited. This requirement covers NIST Security Control 800.53 AC-10.This requirement covers NIST security controls SC-5 (2), SC-5 (3) and AC-10.

Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour><SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0010
Title	Maximum message size per Message Queue and Message Topic
Requirement	The maximum message size shall be configurable.
Status	<validated>
Rationale	For performance and security reasons, the maximum message size has to be configurable. The limit could be configured for all the queues and topics, different queues/topics could have different limits. Finally different groups of queues/topics could have different limits. This level of flexibility allows to fine-tune the trade-off between performance and security needs based on Purple Profile enabled SWIM services (two services could have two different maximum message sizes and time constraints).
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>

Company General Use

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0015
Title	Messages exceeding maximum message size
Requirement	Messages exceeding maximum message size shall be rejected or dropped.
Status	<validated>
Rationale	For security and reliability reasons, it is not allowed to send to a Message Queue or Topic messages exceeding maximum message size.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0020
Title	Message rejected because exceeding maximum message size
Requirement	When rejecting a message because exceeding maximum message size, the sender shall be notified with the reason and the event logged.
Status	<validated>
Rationale	For security and reliability reasons, it is not allowed to send to a Message Queue or Topic messages exceeding maximum message size. When rejecting the message, the sender is notified with the reason and the event logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0025
Title	Message dropped because exceeding maximum message size
Requirement	When dropping a message because exceeding maximum message size the event shall be logged and the message/message dropped event routed according to the applicable context-based routing policy.
Status	<validated>
Rationale	For security and reliability reasons, it is not allowed to send to a Message Queue or Topic messages exceeding maximum message size. When dropping the message, the applicable context-based routing policy requires if and where the message/message dropped event have to be routed to. In all the cases the event has to be logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0030

Title	Overall connection limit
Requirement	The maximum number of allowed concurrent connections shall be configurable.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of concurrent connections has to be configurable. This applies to both Air and Ground Purple Profile SWIM Nodes: - Air SWIM Node: this allows to limit the overall number of connections established by Aircraft applications. - Ground SWIM Node: this allows to limit the overall number of connections established by Aircraft/Air Purple Profile SWIM Nodes and Purple Profile enabled ground applications.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0035
Title	Overall connection limit exceeded

Requirement	When the number of overall maximum connections is exceeded any additional attempt to establish a connection shall be rejected.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of overall connections shall be controlled. This applies to both Air and Ground Purple Profile SWIM Nodes: - Air SWIM Node: this allows to limit the overall number of connections established by Aircraft applications. - Ground SWIM Node: this allows to limit the overall number of connections established by Aircraft/Air Purple Profile SWIM Nodes and Purple Profile enabled ground applications.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0040
Title	Connection establishment rejected because exceeding maximum number of overall connections

Requirement	When rejecting an attempt to establish a connection because exceeding the number of overall maximum connections, the connecting entity shall be notified with the reason and the event logged.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of overall connections shall be controlled. The connecting entity has to be informed about the reason why the connection has been rejected. Furthermore, the event has to be logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0045
Title	Maximum number of concurrent connections per connecting entity
Requirement	The maximum number of allowed concurrent connections per connecting entity shall be configurable.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of concurrent connections per connecting entity has to be configurable.

	This applies to both Air and Ground Purple Profile SWIM Nodes: - Air SWIM Node: this allows to limit the maximum number of concurrent connections established by a single Aircraft application. - Ground SWIM Node: this allows to limit the maximum number of concurrent connections established by a single Aircraft/Air Purple Profile SWIM Node or Purple Profile enabled ground application.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0050
Title	Maximum number of concurrent connections per connecting entity exceeded
Requirement	When the number of maximum allowed concurrent connections per connecting entity is exceeded, any additional attempt to establish a connection shall be rejected.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of concurrent connections per connecting entity shall be controlled. This applies to both Air and Ground Purple Profile SWIM Nodes:

	- Air SWIM Node: this allows to limit the maximum number of concurrent connections established by a single Aircraft application. - Ground SWIM Node: this allows to limit the maximum number of concurrent connections established by a single Aircraft/Air Purple Profile SWIM Node or Purple Profile enabled ground application.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0055
Title	Connection establishment rejected because exceeding maximum number of concurrent connections per connecting entity
Requirement	When rejecting an attempt to establish a connection because exceeding the number of maximum allowed concurrent connections per connecting entity, the connecting entity shall be notified with the reason and the event logged.
Status	<validated>
Rationale	For performance and security reasons, the maximum number of concurrent connections per connecting entity shall be controlled. The connecting entity has to be informed about the reason why the connection has been rejected. Furthermore, the

	event has to be logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0060
Title	Maximum message queue capacity
Requirement	The maximum message queue capacity in terms of size (Mbytes) and in terms of number of messages shall be configured.
Status	<validated>
Rationale	The maximum capacity of queue functionality can be different between distinct products. When the maximum queue is reached it is expected that the reaction of products may differ slightly. This requirement allows to configure the capacity for each Message Queue. This allows to cover different SWIM Service constraints.
Category	<Functional><Security>
Profile Part	<PP Core>

Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0065
Title	Maximum message topic capacity
Requirement	The maximum message topic capacity in terms of size (Mbytes) and in terms of number of messages shall be configured.
Status	<validated>
Rationale	The maximum capacity of topic functionality can be different between distinct products. When the maximum topic is reached it is expected that the reaction of products may differ slightly. This requirement allows to configure the capacity for each Message Topic. This allows to cover different SWIM Service constraints.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication consumer><Publication mediator>
Selfstanding set	<Not applicable>

Company General Use

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0070
Title	Maximum message queue capacity exceeded
Requirement	When the maximum message queue capacity is exceeded any additional attempt to send messages shall be rejected.
Status	<validated>
Rationale	The maximum capacity of queue functionality can be different between distinct products. When the maximum queue capacity is reached it is expected that the reaction of products may differ slightly.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0075
Title	Message send rejected because exceeding the maximum message queue capacity
Requirement	When rejecting an attempt to send a message because exceeding the maximum message queue capacity, the sender shall be notified with the reason and the event logged.
Status	<validated>
Rationale	The maximum capacity of queue functionality can be different between distinct products. When the maximum queue capacity is reached the messages are rejected: the sender has to be informed about the reason and the event has to be logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0080
Title	Maximum message topic capacity exceeded
Requirement	When the maximum message topic capacity is exceeded any additional attempt to publish messages shall be rejected.
Status	<validated>
Rationale	The maximum capacity of topic functionality can be different between distinct products. When the maximum topic capacity is reached it is expected that the reaction of products may differ slightly.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0160.0085
Title	Message publication rejected because exceeding the maximum message topic capacity
Requirement	When rejecting an attempt to publish a message because exceeding the maximum message topic capacity, the publisher shall be notified with the reason and the event logged.
Status	<validated>

Rationale	The maximum capacity of topic functionality can be different between distinct products. When the maximum topic capacity is reached the messages are rejected: the publisher has to be informed about the reason and the event has to be logged.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0105
Title	Monitoring Strategies
Requirement	The SWIM-TI Security shall allow to configure different monitoring strategies according to current security context.
Status	<in progress>
Rationale	Monitoring strategies must suit possible changes in the security context due to increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. For such reason it shall be ensured that different monitoring strategies can be configured and enforced although the definition of such monitoring strategies won't be imposed nor restricted in advance.

	This requirement covers the following NIST security controls: SI-4e, SI-5.A.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Overload Protection Purple Profile

4.3.1.2.9 Security Policy management

[REQ]

Identifier	REQ-17.01-TS-0180.0010
Title	Security policies management via administrative interfaces
Requirement	Security policies shall be defined, updated, enabled and disabled via administrative interfaces.
Status	<validated>
Rationale	Only administrators are authorized to manage security policies.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0015
Title	Authentication policy and digital identity types
Requirement	The Authentication policy shall allow to configure the supported digital identity types.
Status	<validated>
Rationale	At least two digital identities types are supported (normal vs safe mode). The authentication policy allows to properly configure the supported types.
Category	<Functional><Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0020
Title	Static (configuration time) definition of authentication policies
Requirement	The SWIM-TI shall provide mechanisms to statically define authentication policies.
Status	<validated>
Rationale	Authentication policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0025
Title	Dynamic (run time) update of authentication policies
Requirement	The SWIM-TI shall provide mechanisms to dynamically update authentication policies.
Status	<validated>
Rationale	It could happen that authentication policies have to be updated at run-time without restarting system/sub-system.
Category	<Functional><Interface>
Profile Part	<PP Ground>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0030
Title	Per-queue authorization policy
Requirement	The SWIM-TI shall allow to configure per-queue authorization policies.
Status	<validated>
Rationale	For two or more queues different authorization rights could be required.
Category	<Functional><Interface>

Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0035
Title	Per-topic authorization policy
Requirement	The SWIM-TI shall allow to configure per-topic authorization policies.
Status	<validated>
Rationale	For two or more topics different authorization rights could be required.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0040
Title	Role based authorization policies
Requirement	The Authorization policies shall allow to define role based access control rights.
Status	<validated>
Rationale	For a given queue/topic RBAC is required (e.g. senders can only write messages, receiver can only consume messages, only administrators can create a queue, etc.).
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0045
Title	Static (configuration time) definition of authorization policies
Requirement	The SWIM-TI shall provide mechanisms to statically define authorization policies.
Status	<validated>
Rationale	Authorization policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0050
Title	Dynamic (run time) update of authorization policies
Requirement	The SWIM-TI shall provide mechanisms to dynamically update authorization policies.

Status	<validated>
Rationale	It could happen that authorization policies have to be updated (e.g. new authorized consumer) at run-time without restarting system/sub-system.
Category	<Functional><Interface>
Profile Part	<PP Ground>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0055
Title	Cryptographic protocols, algorithms and cipher suites.
Requirement	The Confidentiality, integrity and authenticity policies shall allow to select the allowed cryptographic protocols, algorithms and cipher suites.
Status	<validated>
Rationale	This requirement allows to select only allowed cryptographic protocols, algorithms and cipher suites used for confidentiality, integrity and authenticity ensuring.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0060
Title	Static (configuration time) definition of confidentiality, integrity and authenticity policies
Requirement	The SWIM-TI shall provide mechanisms to statically define confidentiality, integrity and authenticity policies.
Status	<validated>
Rationale	Confidentiality, integrity and authenticity policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0065
Title	Per-queue message screening policy
Requirement	The SWIM-TI shall allow to configure per-queue message screening policies.
Status	<validated>
Rationale	For two or more queues different message screening needs could be required. This includes also disabling message screening for a given queue.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0070
Title	Per-topic message screening policy
Requirement	The SWIM-TI shall allow to configure per-topic message screening policies.
Status	<validated>
Rationale	For two or more topics different message screening needs could be required. This includes also disabling message screening for a given topic.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0075
Title	Static (configuration time) definition of message screening policies
Requirement	The SWIM-TI shall provide mechanisms to statically define message screening policies.
Status	<validated>

Rationale	Message screening policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0080
Title	Dynamic (run time) update of message screening policies
Requirement	The SWIM-TI shall provide mechanisms to dynamically update message screening policies.
Status	<validated>
Rationale	It could happen that message screening policies have to be updated at run-time without restarting system/sub-system.
Category	<Functional><Interface>
Profile Part	<PP Ground>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0085
Title	Static (configuration time) definition of overload protection policies
Requirement	The SWIM-TI shall provide mechanisms to statically define overload protection policies.
Status	<validated>
Rationale	Overload protection policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0090
Title	Dynamic (run time) update of overload protection policies
Requirement	The SWIM-TI shall provide mechanisms to dynamically update overload protection policies.
Status	<validated>
Rationale	It could happen that overload protection policies have to be updated at run-time without restarting system/sub-system.
Category	<Functional><Interface>
Profile Part	<PP Ground>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0110.0100
Title	Audit Policy Minimal Content
Requirement	The SWIM-TI Audit Policy shall at least include the following information: - The information which need to be recorded, - The user roles that must be provided with audit records, - The frequency of reporting or event type triggering the audit.
Status	<in progress>
Rationale	To enable the auditing process every security related event needs to be logged with all the additional information specified by the applicable Audit Policy. This requirement covers the following NIST security controls: SI-4e, SI-4 g.
Category	<Functional><Security>
Profile Part	<PP Core>
Domain of Interest	<Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0180.0095
Title	Static (configuration time) definition of audit policies

Requirement	The SWIM-TI shall provide mechanisms to statically define audit policies.
Status	<in progress>
Rationale	Audit policies have to be configured and enabled.
Category	<Functional><Interface>
Profile Part	<PP Core>
Domain of Interest	<Governance><ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Security Policy Management Purple Profile

4.3.1.2.10 Crosscutting

[REQ]

Identifier	REQ-17.01-TS-0110.0255
Title	SWIM-TI support for incident reporting
Requirement	The SWIM-TI Security shall include a functionality for reporting the handling of the following Security Incidents: + Denial of Service. + Intrusion. + Malicious or unauthorized software installation. + Reconnaissance (e.g. port scanning).

	+ Physical damage. + Information compromise. + Software failure (with security implications).
Status	<in progress>
Rationale	It is important to monitor any incidents that may have an impact on security. This requirement ensures that the SWIM Technical Infrastructure provides a functionality aiming at reporting the handling of these incidents. This requirement covers NIST security controls: AU-2 a, IR-5, SI-4b, SI-4g, SI-11a.
Category	<Functional><HMI><Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

4.3.2 Design and Construction Constraints

This section includes design and construction constraints requirements representing constraints driving the technical view design and specification.

[REQ]

Identifier	REQ-17.01-TS-0450.0015
Title	SWIM-TI Messaging efficient use of Purple Profile Datalink
Requirement	The SWIM-TI Messaging shall efficiently use Air-Ground Datalink resources.
Status	<validated>
Rationale	To contribute to the cost effectiveness goal of SESAR. For example this may rely on minimization of the number of link and connections between A/C and Ground.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0065
Title	SWIM-TI Messaging Only A/C Initiated TCP/IP connections

Requirement	The SWIM-TI Messaging shall be designed in the way that Purple Profile TCP/IP connections are only initiated from A/C side.
Status	<validated>
Rationale	The aircraft shall have open communication ports to trusted ground systems only. In that case, TCP/IP connections need to be initiated by the aircraft. TCP/IP session establishment. This mechanism only apply at the TCP/IP level. Only TCP/IP must be initiated by the Aircraft, for avoiding that malicious ground system can directly access Aircraft.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA><Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0080
Title	SWIM infrastructure design and onboard resources
Requirement	Design of the air/ground SWIM infrastructure shall minimize computational complexity onboard and data link bandwidth consumption.

Status	<validated>
Rationale	Effective use of aircraft resources.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0300
Title	Configuration management of Installed Air Purple Profile SWIM Node components
Requirement	Installed Air Purple Profile SWIM Node components configuration shall be managed under the aircraft type design configuration.
Status	<validated>
Rationale	Installed Air Purple Profile SWIM Node components are considered as an aircraft part. Aircraft parts' maintenance and configuration control is operated under the Air transport operator Continuing Airworthiness Management Organization (CAMO) per EASA EU regulation (Part M, Part 145). Per EASA AMC 20-25, an EFB host platform installed in the aircraft is considered as an aircraft part, covered, thus, by the aircraft airworthiness approval.
Category	<Maintenability>

Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0305
Title	Configuration management of portable Air Purple Profile SWIM Node components
Requirement	Non installed Air Purple Profile SWIM Node components configuration shall be managed under the operator's EFB administrator responsibility.
Status	<validated>
Rationale	Per EASA AMC 20-25, portable EFB host platform used on the flight deck is not part of the certified aircraft configuration. The EFB administrator is responsible for the complete system with appropriate authority within the operator's management structure.
Category	<Maintenability>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0310
Title	Installed Air Purple Profile SWIM Node maintenance
Requirement	Air Purple Profile SWIM Node maintenance, including configuration changes, on installed equipment shall be conducted on ground only.
Status	<validated>
Rationale	Aircraft's equipment parts are maintained under operator CAMO.
Category	<Maintenability>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0315
Title	Portable Air Purple Profile SWIM Node maintenance
Requirement	Air Purple Profile SWIM Node maintenance, including configuration changes, on portable equipment shall be conducted on operator premises only.
Status	<validated>
Rationale	Portable equipment, not part of aircraft configuration, is maintained under the operator responsibility.
Category	<Maintenability>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0020
Title	Uplink and Downlink exchanges support

Requirement	The SWIM-TI Messaging shall allow ground-to-air (uplink) and air-to-ground (downlink) information distribution.
Status	<validated>
Rationale	Two main information exchanges directions needed for the A(G SWIM.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0025
Title	Data link modes for information uplink
Requirement	The SWIM-TI Messaging shall allow broadcast, demand and contract data link modes for ground-to-air (uplink) information distribution.
Status	<validated>
Rationale	ED-151 defined data link modes supported for uplink information distribution.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>

Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0030
Title	Data link modes for information downlink
Requirement	The SWIM-TI Messaging shall allow broadcast, demand and contract data link modes for air-to-ground (downlink) information distribution.
Status	<validated>
Rationale	ED-151 defined data link modes supported for downlink information distribution.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0035
Title	Broadcast data link mode (downlink and uplink) over PSPUSH-MEP.
Requirement	The broadcast data link mode (downlink and uplink) information distribution shall be realized over PSPUSH-MEP.
Status	<validated>
Rationale	The profile specification describes how PS MEP is realized over the Air-Ground SWIM infrastructure. The broadcast data link mode is realized over this MEP.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0045
Title	Demand data link mode (downlink and uplink) over FDRR-MEP.
Requirement	The demand data link mode (downlink and uplink) information distribution shall be realized over FDRR-MEP.
Status	<validated>
Rationale	The profile specification describes how FDRR-MEP is realized over the Air-Ground SWIM infrastructure. One possible option to realize the demand data link mode is over this MEP. This is the recommended option.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0055
Title	Demand data link mode (downlink and uplink) either over the composition of FDRR-MEP and PS*-MEP or over FDRMR-MEP.
Requirement	The contract data link mode (downlink and uplink) information distribution shall be

	realized either over the composition of FDRR-MEP and PS*-MEP or over FDRMR-MEP.
Status	<validated>
Rationale	The profile specification describes how FDRR-MEP and PS*-MEP are realized over the Air-Ground SWIM infrastructure. The demand data link mode (downlink and uplink) may be realized over one of the two following options: - composition of FDRR-MEP and PS*-MEP. - FDRMR-MEP.
Category	<Design>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

4.3.3 Reliability requirements

This section includes infrastructure reliability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with reliability NFR sub-characteristics described in ISO/IEC 25010:2011: maturity, availability, fault tolerance and recoverability.

Operations relying on aircraft software applications that do not require airworthiness approval, but require evaluation and operation approval assessment, must demonstrate the fidelity and reliability of the system. To do so, according to EASA EU-OPS Part Cat (CAT.GE.MPA.180), reliability assessment and suitable means of mitigation against failure or malfunction are required.

4.3.3.1 Maturity

Requirements concerning this sub-characteristic have not been identified during SESAR 2020 programme. This sub-characteristic should be further investigated according to the evolution of this technical specification (e.g. industrialization, deployment, standardization, etc.).

4.3.3.2 Availability

[REQ]

Identifier	REQ-17.01-TS-0380.0010
Title	Air and Ground SWIM Nodes availability
Requirement	The SWIM Node availability shall be greater than or equal to the highest availability required for Purple Profile enabled SWIM services consumed/provided through it.
Status	<in progress>
Rationale	The availability of SWIM Nodes depends on the availability required for Purple Profile enabled SWIM services consumed or provided through them. ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services availability and continuity requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different availability requirements. - For a given candidate PP enabled SWIM service, the availability requirements could be different depending on the operational environment (enroute, terminal, airport). - A given SWIM Node (Air or Ground) could be used to consume or/and provide several SWIM services each with different availability requirements. Taking into account the above, it does not make sense to provide quantitative availability requirements with several figures. The provided requirement establishes the dependency with the availability of Purple Profile enabled SWIM services and SWIM Node (Air and/or Ground): the appropriate SWIM Node availability figure is identified when the set of Purple Profile enabled SWIM services operated ever the SWIM infrastructure is available.

Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0380.0015
Title	Air-Ground SWIM Nodes pair availability
Requirement	The availability of Air-Ground SWIM Nodes pair shall be greater than or equal to the highest availability required for Purple Profile enabled SWIM services consumed/provided through it.
Status	<in progress>
Rationale	The availability of SWIM Nodes depends on the availability required for Purple Profile enabled SWIM services consumed or provided through them. ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services availability and continuity requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different availability requirements. - For a given candidate PP enabled SWIM service, the availability requirements could be different depending on the operational environment (enroute, terminal, airport). - A given SWIM Node (Air or Ground) could be used to consume or/and provide

	several SWIM services each with different availability requirements. Taking into account the above, it does not make sense to provide quantitative availability requirements with several figures. The provided requirement establishes the dependency with the availability of Purple Profile enabled SWIM services and Air-Ground SWIM Nodes pair: the appropriate SWIM Nodes pair availability figure is identified when the set of Purple Profile enabled SWIM services operated ever the SWIM infrastructure is available. Availability requirement at Air-Ground SWIM Nodes pair level is provided for two purposes: a) end to end Purple Profile enabled SWIM service availability and b) indirect availability requirement for the Air/Ground network infrastructure.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

4.3.3.3 Recoverability

[REQ]

Identifier	REQ-17.01-TS-0390.0020
Title	Air and Ground SWIM Nodes continuous unavailability
Requirement	The SWIM Node continuous unavailability shall be less than or equal to the lowest continuous unavailability required for Purple Profile enabled SWIM services consumed/provided through it.
Status	<in progress>

Rationale	Continuity of SWIM Nodes depends on the continuity required for Purple Profile enabled SWIM services consumed or provided through them. ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services availability and continuity requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different continuity requirements. - For a given candidate PP enabled SWIM service, the continuity requirements could be different depending on the operational environment (enroute, terminal, airport). - A given SWIM Node (Air or Ground) could be used to consume or/and provide several SWIM services each with different continuity requirements. Taking into account the above, it does not make sense to provide quantitative continuity requirements with several figures. The provided requirement establishes the dependency with the continuity of Purple Profile enabled SWIM services and SWIM Node (Air and/or Ground): the appropriate SWIM Node continuous unavailability figure is identified when the set of Purple Profile enabled SWIM services operated ever the SWIM infrastructure is available. It is anticipated that also additional requirements concerning (e.g.) planned outages scheduling, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) should be analyzed taking into account relevant Purple Profile enabled SWIM services level requirements, business impact, threat and risk analysis. These are aspects documented (when required) in the business continuity planning.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0390.0025
Title	Air-Ground SWIM Nodes pair continuous unavailability
Requirement	The continuous unavailability of Air-Ground SWIM Nodes pair shall be less than or equal to the lowest continuous unavailability required for Purple Profile enabled SWIM services consumed/provided through it.
Status	<in progress>
Rationale	Continuity of SWIM Nodes depends on the continuity required for Purple Profile enabled SWIM services consumed or provided through them. ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services availability and continuity requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different continuity requirements. - For a given candidate PP enabled SWIM service, the continuity requirements could be different depending on the operational environment (enroute, terminal, airport). - A given SWIM Node (Air or Ground) could be used to consume or/and provide several SWIM services each with different continuity requirements. Taking into account the above, it does not make sense to provide quantitative continuity requirements with several figures. The provided requirement establishes the dependency with the continuity of Purple Profile enabled SWIM services and Air-Ground SWIM Nodes pair: the appropriate SWIM Nodes pair continuous unavailability figure is identified when the set of Purple Profile enabled SWIM services operated ever the SWIM infrastructure is available. Continuous unavailability requirement at Air-Ground SWIM Nodes pair level is provided for two purposes: a) end to end Purple Profile enabled SWIM service continuity and b) indirect continuous unavailability requirement for the Air/Ground network infrastructure. It is anticipated that also additional requirements concerning (e.g.) planned outages scheduling, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) should be analyzed taking into account relevant Purple Profile enabled SWIM services level requirements, business impact, threat and risk analysis. These are aspects documented (when required) in the business continuity planning.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>

Company General Use

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0390.0030
Title	AMQP 1.0 based instantiation of At-Most-Once point-to-point delivery guarantee
Requirement	AMQP 1.0 based instantiation of At-Most-Once point-to-point delivery guarantee shall be as follows: + Settling - higher level messaging functionality over AMQP 1.0 standard settling transport level mechanism to configure and enforce the settling strategy. - sending entity must settle the delivery before sending the message. + Link recovery: - None. + Durability: - Non-durable message durability. - Either Non-Durable or Volatile MQ, MT and Subscription handler durability. - Either Non-Durable or Durable Subscription durability.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of At-Most-Once point-to-point delivery guarantee has to be realized. Taking into account that this QoS does not guarantee that messages are not lost there are no obligations for the message, MQ and MT durability QoSs. However, in order to save messaging

	resources, durability QoSs options are restricted. Relationships between mentioned messaging entities and SWIM Nodes, and SWIM enabled applications are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0065

[REQ]

Identifier	REQ-17.01-TS-0390.0035
Title	AMQP 1.0 based instantiation of At-Least-Once point-to-point delivery guarantee
Requirement	AMQP 1.0 based instantiation of At-Least-Once point-to-point delivery guarantee shall be as follows: + Settling - higher level messaging functionality over AMQP 1.0 standard settling transport level mechanism to configure and enforce the settling strategy. - sending entity (Sender, Publisher) must not settle the delivery before sending the message. - receiving entity (MQ, MT, Receiver, Subscriber) must settle the delivery immediately

	upon processing the message. + Link recovery: - higher level messaging functionality over AMQP 1.0 standard link resume transport level mechanism. - link recovery is not initiated by MQ, MT and Subscription handler messaging entities. - link recovery must be initiated by the sender, receiver, publisher and subscriber messaging entities. - link recovery automatic retry attempted according to policy. + Durability: - Durable Message durability. - Durable MQ, MT and Subscription handler durability. - Either Non-Durable or Durable Subscription durability.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of At-Least-Once point-to-point delivery guarantee has to be realized. Relationships between mentioned messaging entities and SWIM Nodes, and SWIM enabled applications are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0070

[REQ]

Identifier	REQ-17.01-TS-0390.0040
Title	AMQP 1.0 based instantiation of Exactly-Once point-to-point delivery guarantee
Requirement	AMQP 1.0 based instantiation of Exactly-Once point-to-point delivery guarantee shall be as follows: + Settling - higher level messaging functionality over AMQP 1.0 standard settling transport level mechanism to configure and enforce the settling strategy. - sending entity (Sender, Publisher) must settle the delivery when the receiver reaches a terminal state. - receiving entity (MQ, MT, Receiver, Subscriber) must settle the delivery when the sending entity settles. - higher level messaging functionalities receiving entity side to detect and filter-out duplicated messages (UUID for message-id). + Link recovery: - higher level messaging functionality over AMQP 1.0 standard link resume transport level mechanism. - link recovery is not initiated by MQ, MT and Subscription handler messaging entities. - link recovery must be initiated by the sender, receiver, publisher and subscriber messaging entities. - link recovery automatic retry attempted according to policy. + Durability: - Durable Message durability. - Durable MQ, MT and Subscription handler durability. - Either Non-Durable or Durable Subscription durability.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Exactly-Once point-to-point delivery guarantee has to be realized. Relationships between mentioned messaging entities and SWIM Nodes, and SWIM

	enabled applications are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0071

[REQ]

Identifier	REQ-17.01-TS-0390.0045
Title	Air SWIM Node - Ground SWIM Node AMQP connections delivery guarantees
Requirement	For a given AMQP connection, the message passing between two directly connected Air and Ground SWIM Nodes shall have either At-Most-Once or At-Least-Once or Exactly-Once point-to-point delivery guarantee depending on the required end-to-end delivery guarantees of the Purple Profile enabled SWIM Services concerning that AMQP connection.
Status	<validated>
Rationale	The Air SWIM Node establishes connection(s) towards Ground SWIM Node(s) in order to be able to federate the MEPs. This is the connection used to create the session and the link concerning “Internal service bindings”. Depending of MQs segregation (used for more than one services, etc.) this interfacing layer has to behave according to the chosen delivery guarantees for the specific/group of Purple Profile enabled SWIM service/s.

	Furthermore, it is not allowed to have "No delivery guarantees" QoS for Air SWIM Node - Ground SWIM Node connections.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0390.0050
Title	AMQP 1.0 based instantiation of At-Most-Once end-to-end delivery guarantee
Requirement	AMQP 1.0 based instantiation of At-Most-Once end-to-end delivery guarantee shall be as follows: - higher level messaging functionality over AMQP 1.0 standard. - point-to-point delivery guarantee for all the directly connected messaging entities set to At-Most-Once.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of At-Most-Once end-to-end delivery guarantee has to be realized. Sender and receiver (publisher and subscriber) messaging entities are not directly connected: end-to-end sender-receiver (publisher-subscriber) message distribution is through the MQ (MT). In order to meet end-to-end delivery guarantees needs, the point-to-point delivery guarantees for both Sender-MQ (Publisher-MT) and MQ-

	Receiver (MT-Subscriber) connections have to be properly set. Furthermore, taking into account that for a given Purple Profile enabled SWIM service, message distribution (MQ/MT) is federated via AMQP distribution nodes (Air SWIM Node - Ground SWIM Node pair) a third connection type exists for which proper point-to-point delivery guarantee has to be set. Relationships between messaging entities and SWIM Nodes, SWIM enabled applications and SWIM services are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0080

[REQ]

Identifier	REQ-17.01-TS-0390.0055
Title	AMQP 1.0 based instantiation of At-Least-Once end-to-end delivery guarantee
Requirement	AMQP 1.0 based instantiation of At-Least-Once end-to-end delivery guarantee shall be as follows: - higher level messaging functionality over AMQP 1.0 standard. - point-to-point delivery guarantee for all the directly connected messaging entities set to At-Least-Once.

Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of At-Least-Once end-to-end delivery guarantee has to be realized. Sender and receiver (publisher and subscriber) messaging entities are not directly connected: end-to-end sender-receiver (publisher-subscriber) message distribution is through the MQ (MT). In order to meet end-to-end delivery guarantees needs, the point-to-point delivery guarantees for both Sender-MQ (Publisher-MT) and MQ-Receiver (MT-Subscriber) connections have to be properly set. Furthermore, taking into account that for a given Purple Profile enabled SWIM service, message distribution (MQ/MT) is federated via AMQP distribution nodes (Air SWIM Node - Ground SWIM Node pair) a third connection type exists for which proper point-to-point delivery guarantee has to be set. Relationships between messaging entities and SWIM Nodes, SWIM enabled applications and SWIM services are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0085

[REQ]

Identifier	REQ-17.01-TS-0390.0060

Title	AMQP 1.0 based instantiation of Exactly-Once end-to-end delivery guarantee
Requirement	AMQP 1.0 based instantiation of Exactly-Once end-to-end delivery guarantee shall be as follows: - higher level messaging functionality over AMQP 1.0 standard. - point-to-point delivery guarantee for all the directly connected messaging entities set to Exactly-Once.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Exactly-Once end-to-end delivery guarantee has to be realized. Sender and receiver (publisher and subscriber) messaging entities are not directly connected: end-to-end sender-receiver (publisher-subscriber) message distribution is through the MQ (MT). In order to met end-to-end delivery guarantees needs, the point-to-point delivery guarantees for both Sender-MQ (Publisher-MT) and MQ-Receiver (MT-Subscriber) connections have to be properly set. Furthermore, taking into account that for a given Purple Profile enabled SWIM service, message distribution (MQ/MT) is federated via AMQP distribution nodes (Air SWIM Node - Ground SWIM Node pair) a third connection type exists for which proper point-to-point delivery guarantee has to be set. Relationships between messaging entities and SWIM Nodes, SWIM enabled applications and SWIM services are documented in the technical specification (technical viewpoint).
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0086

[REQ]

Identifier	REQ-17.01-TS-0390.0065
Title	AMQP 1.0 based instantiation of Message Lifespan/Lifetime QoS
Requirement	AMQP 1.0 based instantiation of Message Lifespan/Lifetime QoS shall be as follows: - higher level messaging functionality over AMQP 1.0 standard to handle (context-based filter & route) expired messages. - AMQP header ttl and AMQP Bare Message Standard properties absolute-expiry-time fields have to be set.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Message Lifespan/Lifetime QoS has to be realized. Expired messages are filtered out and routed according to the applicable context-based routing policy.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0005

[REQ]

Identifier	REQ-17.01-TS-0390.0070
Title	Handling of messages with undefined expiration time
Requirement	When receiving a message with undefined expiration time, the SWIM Node shall either reject it or add the default expiration time.
Status	<validated>
Rationale	In order to avoid message starvation in MQ and MT (resources saving) messages which will not expire are not allowed. This design decision is also coherent with the fact that advisory information (AI/MET) have typically a limited lifetime. The decision to reject the message or to add the default expiration time could be based on local messaging policies.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0390.0075
Title	AMQP 1.0 based instantiation of Non-Temporary Message Queue and Message Topic

	Lifespan/Lifetime QoS
Requirement	AMQP 1.0 based instantiation of Non-Temporary Message Queue and Message Topic Lifespan/Lifetime QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - target and source terminus terminus-expiry-policy set to never.
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Non-Temporary Message Queue and Message Topic Lifespan/Lifetime QoS should be realized. Furthermore, for completeness it is important to notice that: - MQ and MT lifecycle is management via administrative interfaces. - Temporary MQ and MT are not allowed.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0010
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0015

[REQ]

Identifier	REQ-17.01-TS-0390.0080
Title	AMQP 1.0 based instantiation of Subscription with zero/unspecified lifespan QoS
Requirement	AMQP 1.0 based instantiation of Subscription with zero/unspecified lifespan QoS shall be as follows: - higher level messaging functionality over AMQP 1.0 standard. - subscription management semantics and federation in accordance with the technical viewpoint. - subscription management messages in accordance with the provided XSD. - subscription management AMQP messages in accordance with the technical viewpoint.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Subscription with zero/unspecified lifespan QoS has to be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0020

[REQ]

Identifier	REQ-17.01-TS-0390.0085
Title	AMQP 1.0 based instantiation of Subscription with non-zero/specified lifespan QoS
Requirement	AMQP 1.0 based instantiation of Subscription with non-zero/specified lifespan QoS shall be as follows: - higher level messaging functionality over AMQP 1.0 standard. - subscription management semantics and federation in accordance with the technical viewpoint. - subscription management messages in accordance with the provided XSD. - subscription management AMQP messages in accordance with the technical viewpoint.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Subscription with non-zero/specified lifespan QoS has to be realized.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0021

[REQ]

Identifier	REQ-17.01-TS-0390.0090
Title	Durability messaging QoS and limited non-volatile memories resources
Requirement	SWIM-TI Messaging durability QoS shall remain compatible with aircraft's available resources.
Status	<validated>
Rationale	Capacity to survive a transient/permanent failure depends on data protection. SEU protected Non-volatile Memories resource is limited on avionics components. Failure of Durable services mapped on on-board unprotected Non-volatile Memories should be anticipated.
Category	<Reliability><Performance>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0390.0095
Title	AMQP 1.0 based instantiation of Durable message durability QoS
Requirement	AMQP 1.0 based instantiation of Durable message durability QoS shall be as follows: - the standard AMQP header durable field has to be set to TRUE.
Status	<validated>

Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Durable message durability QoS has to be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0040

[REQ]

Identifier	REQ-17.01-TS-0390.0100
Title	AMQP 1.0 based instantiation of Non-Durable message durability QoS
Requirement	AMQP 1.0 based instantiation of Non-Durable message durability QoS shall be as follows: - the standard AMQP header durable field has to be set to FALSE.
Status	<validated>
Rationale	This requirement aims at constraining how the AMQP 1.0 based instantiation of Non-Durable message durability QoS has to be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0040

[REQ]

Identifier	REQ-17.01-TS-0390.0105
Title	AMQP 1.0 based instantiation of Non-Durable Message Queue and Message Topic durability QoS
Requirement	AMQP 1.0 based instantiation of Non-Durable Message Queue and Message Topic durability QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - terminus durability set to 0 .
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Non-Durable Message Queue and Message Topic durability QoS should be realized. This QoS makes sense only if a non-durable message QoS is required at message level.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0045
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0050

[REQ]

Identifier	REQ-17.01-TS-0390.0110
Title	AMQP 1.0 based instantiation of Volatile Message Queue, Message Topic and and Subscription handler durability QoS
Requirement	AMQP 1.0 based instantiation of Volatile Message Queue, Message Topic and Subscription handler durability QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - terminus durability set to 1 .
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Volatile Message Queue, Message Topic and Subscription handler durability QoS should be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0045
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0050
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0060

[REQ]

Identifier	REQ-17.01-TS-0390.0115
Title	AMQP 1.0 based instantiation of Durable Message Queue, Message Topic and Subscription handler durability QoS
Requirement	AMQP 1.0 based instantiation of Durable Message Queue, Message Topic and Subscription handler durability QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - terminus durability set to 2.
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Durable Message Queue, Message Topic and Subscription handler durability QoS should be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0045
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0050
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0061

[REQ]

Identifier	REQ-17.01-TS-0390.0120
Title	AMQP 1.0 based instantiation of Non-Durable Subscription durability QoS
Requirement	AMQP 1.0 based instantiation of Non-Durable Subscription durability QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - terminus expiry policy set to link-detach or session-end or connection-close.
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Non-Durable Subscription durability QoS should be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0055

[REQ]

Identifier	REQ-17.01-TS-0390.0125
Title	AMQP 1.0 based instantiation of Durable Subscription durability QoS
Requirement	AMQP 1.0 based instantiation of Durable Subscription durability QoS should be as follows: - higher level messaging functionality over AMQP 1.0 standard. - terminus expiry policy set to never.
Status	<validated>
Rationale	This requirement aims at providing recommendations on how the AMQP 1.0 based instantiation of Durable Subscription durability QoS should be realized.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0040.0055

4.3.3.4 Fault tolerance

[REQ]

Identifier	REQ-17.01-TS-0400.0010
Title	Impact of Air Purple Profile SWIM Node failure on Aircraft Dispatch
Requirement	Failure of Air Purple Profile SWIM Node shall not impair Aircraft dispatch.
Status	<validated>
Rationale	MMEL Rectification Interval Category for the AIR AG SWIM PP system is “D” (Items in this category shall be rectified within 120 calendar days). “D” category is assumed for the Air Purple Profile SWIM Node installation, as meeting the following criteria: 1. The absence of the item does not adversely affect crew member's workload; 2. The crew members do not rely on the function of that item on a routine or continuous basis; and 3. The crew members' training, subsequent habit patterns and procedures do not rely on the use of that item.
Category	<Reliability>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0015
Title	Internal Ground SWIM Node fault isolation and containment
Requirement	The Fault tolerance solution of the Ground SWIM Node shall provide internal faults isolation and containment.
Status	<validated>
Rationale	Basic characteristics of fault tolerance solutions to be further detailed in more general High Availability solutions definition.
Category	<Reliability>
Profile Part	<PP Ground>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0020
Title	At-Least-Once and Exactly-Once delivery guarantees and non-nominal cases

Requirement	Automatic retry after connection error or unexpected link detach or unexpected end of session or unexpected close of connection, shall be attempted according to the retry policy and when At-Least-Once or Exactly-Once delivery guarantees are required.
Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy and initiated by the peer initiating the connection/reconnection. In particular, reconnection and retry policies concern: + Application layer: - Purple Profile enabled aircraft and ground applications connecting to SWIM Nodes. + SWIM-TI layer: - Air SWIM Node connecting to Ground SWIM Node(s). - Ground SWIM Node connecting to ground SWIM service(s). Automatic retry mechanisms are necessary but not sufficient condition for these delivery guarantees. In particular also retries may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc. Depending on the criticality, events like “Message not delivered event due to reconnection establishment failure when At-Least-Once delivery guarantee is required” should be logged and traced. Furthermore, the event should be also reported (e.g. monitoring capabilities).
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0025
Title	At-Least-Once and Exactly-Once delivery guarantees and Message not delivered failure
Requirement	Message not delivered failure shall be logged, traced and reported to monitoring capabilities when At-Least-Once or Exactly-Once delivery guarantees are required.
Status	<validated>
Rationale	Automatic retry mechanisms are necessary but not sufficient condition for these delivery guarantees. In particular also retries may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0030
Title	At-Least-Once and Exactly-Once delivery guarantees and Message dropped failure
Requirement	Message dropped failure shall be logged, traced and reported to monitoring capabilities when At-Least-Once or Exactly-Once delivery guarantees are required.
Status	<validated>
Rationale	Automatic retry mechanisms are necessary but not sufficient condition for these delivery guarantees. In particular also retries may fail due to unrecoverable faults like network isolation, maximum number of retries, maximum number of connection, maximum message/queue size, etc.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0035
Title	Retry policy parameters
Requirement	The retry policy shall allow to configure following parameters: + Max reconnection attempts: - The maximum number of reconnection attempts allowed before reporting the

	failure. + Initial Reconnection/Retry delay: - The amount of time the connecting peer waits before the first attempt to reconnect to a remote peer. + Reconnection/retry delay: - The amount of time between successive reconnection attempts. + Exponential back-off: - Use of exponential back-off algorithm in the successive reconnection attempts + Connection URIs: - One or more URIs to connect to in case of connection/reconnect failure. - URIs are either logical names or physical addresses (IP + port).
Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. This requirement provides the minimum set of information/parameters configurable via the policy. These parameters are widely supported out of the box by most AMQP-compliant messaging products.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0040
Title	Max reconnection attempts retry policy parameter default value
Requirement	The Max reconnection attempts parameter of the retry policy shall allow a default value for disabling the retry.
Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. This requirement provides constraints concerning the Max reconnection attempts retry policy parameter.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0045
Title	Max reconnection attempts retry policy parameter maximum value

Requirement	The Max reconnection attempts parameter of the retry policy should not be configured to retry forever.
Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. This requirement provides constraints concerning the Max reconnection attempts retry policy parameter.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0050
Title	Exponential back-off retry policy parameter configuration
Requirement	The Exponential back-off parameter of the retry policy shall allow to configure following sub-parameters: - enable/disable the use of the exponential back-off algorithm. When disable the reconnection delay between successive reconnection attempts remains constant (retry delay parameter) - the multiplier for growing successive reconnection attempts according to the

	algorithm. - maximum reconnection delay to limit the maximum delay evaluated by the algorithm.
Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. This requirement provides constraints concerning the Exponential back-off retry policy parameter.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0055
Title	Connection URIs retry policy parameter configuration
Requirement	The Connection URIs parameter of the retry policy shall allow to configure the following order strategies to be used to try the available URIs: - list based order, - randomly.

Status	<validated>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. The Connection URIs retry policy parameter allows to provide one or more URIs to connect to in case of connection/reconnect failure. These URIs could be logical names and physical addresses (IP + port). In case a single URI is provided the reconnection attempts will use the same URI. This could be a logical name mapped to one or more physical addresses concerning different replicas. How two or more replicas should be synchronized is not specified: an open and standard (AMQP) based approach is recommended. This requirement provides constraints concerning the order strategies to be used to try the available URIs.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0060
Title	Run-time update of the Connection URIs retry policy parameter
Requirement	The retry mechanism shall allow to update the connection URIs parameter of the retry policy at run-time without restarting the software system/sub-system.

Status	<in progress>
Rationale	For both At-Least-Once or Exactly-Once delivery guarantees reconnection and retry mechanisms are required (unexpected detach of link, unexpected end of session or unexpected close of connection). These mechanisms are configured via retry policy. The Connection URIs retry policy parameter allows to provide one or more URIs to connect to in case of connection/reconnect failure. These URIs could be logical names and physical addresses (IP + port). In case a single URI is provided the reconnection attempts will use the same URI. This could be a logical name mapped to one or more physical addresses concerning different replicas. How two or more replicas should be synchronized is not specified: an open and standard (AMQP) based approach is recommended. This requirement provides constraints concerning the sun-time update of the available URIs. There are AMQP 1.0 core, legacy and draft AMQP based standards/mechanism (e.g. AMQP 1.0 core “amqp:connection:redirect” error, draft OASIS “Connection Failover Properties”) allowing the “connection” server to provide the client with available alternate URIs. These solutions are not mandated by this specification. However, standard AMQP 1.0 amqp:connection:redirect connection error (§2.8.16) and amqp:link:redirect (§2.8.18) may be used.
Category	<Reliability>
Profile Part	<PP Ground Advanced><PP Air Advanced>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0400.0065

Title	Per AMQP connection configurability of AMQP idle-time-out
Requirement	The AMQP idle-time-out shall be configurable per AMQP connections.
Status	<validated>
Rationale	A variety of anomalies can cause a hang status in one of the connecting peer. In some cases such hangs cannot be undone by the action of a single peer and may exclusively block resources at the side of the other peer (e.g. connection closed by server peer but in the TCP TIME_WAIT state). Connection-oriented messaging protocols may support time out mechanisms on top of timeout mechanisms already present in underlying transport protocols such as TCP. In such case time-out mechanisms at the level of the messaging protocol are useful to detect in a timely manner an anomaly that could be hidden for a long time by an underlying complex of transport and network protocols. Two mechanisms with low overhead complement each other in the ability to detect such cases and to free exclusively blocked resources: the idle-time-out in the AMQP 1.0 core open performative (aka “heartbeat”) and the “Keep Alive” mechanism at TCP level.
Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0260.0010

Title	AMQP idle-time-out lower and upper bounds
Requirement	The AMQP idle-time-out shall not be less than 60000 milliseconds and not higher than 300000 milliseconds.
Status	<validated>
Rationale	A variety of anomalies can cause a hang status in one of the connecting peer. In some cases such hangs cannot be undone by the action of a single peer and may exclusively block resources at the side of the other peer (e.g. connection closed by server peer but in the TCP TIME_WAIT state). Connection-oriented messaging protocols may support time out mechanisms on top of timeout mechanisms already present in underlying transport protocols such as TCP. In such case time-out mechanisms at the level of the messaging protocol are useful to detect in a timely manner an anomaly that could be hidden for a long time by an underlying complex of transport and network protocols. Two mechanisms with low overhead complement each other in the ability to detect such cases and to free exclusively blocked resources: the idle-time-out in the AMQP 1.0 core open performative (aka “heartbeat”) and the “Keep Alive” mechanism at TCP level. As the “Keep Alive” mechanism at TCP level may not yield the desired and/or expected effect it is necessary to be able to switch it off. Furthermore, a number of behaviors at TCP level are derived from the Maximum Segment Lifetime (MSL) for TCP (RFC 793, default value is 2 minutes) including intentionally keeping quiet for a while (TCP Quiet Time concept, MSL duration), as well as the timeout on TIME_WAIT state, which is set by default at 2 * MSL (i.e. 4 minutes by default), as well the upper bound for RTO (Retransmission Timeout as in RFC 793) (2 * MSL, i.e. 4 minutes by default). While it is expecting that the software environment will allow to properly configure (when needed) different values for MSL (2 minutes or less) and RTO (significantly below the default upper bound of 4 minutes), it makes sense to identify lower and upper bounds for the AMQP idle-time-out: - Too short idle-time-out could lead to excessive load and unnecessary clean-up needing retries. - Too long idle-time-out could lead to too long blocking of resources in case of anomaly. The upper bound could be evaluated starting from default MSL and RTO: an AMQP idle-time-out of 5 minutes (2 * MSL + 1 minute or 300000 milliseconds) provides sufficient time to lower protocol layers to clean up, recover and/or get back into a known and controlled state. If after 5 minutes this is not case, then the AMQP 1.0 idle-time-out will kick in and may help to detect and recover from such states. The lower bound could be evaluated taking into account lifetime of messages: a lower bound shorter than the message expiration time introduces generate unnecessary traffic. Advisory SWIM services concern aeronautical and weather data with different lifetime. Taking into account that it is not possible to have an exhaustive analysis of all the candidate Purple Profile enabled SWIM services, a lower bound of 1 minute (60000 milliseconds) is considered.

Category	<Reliability>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

4.3.4 Performance requirements

This section includes performance efficiency requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with performance efficiency NFR sub-characteristics described in ISO/IEC 25010:2011: time behaviour, resource utilization and capacity.

4.3.4.1 Resource utilization

Requirements concerning this sub-characteristic have not been identified during SESAR 2020 programme. This sub-characteristic should be further investigated according to the evolution of this technical specification (e.g. industrialization, deployment, standardization, etc.). It is however anticipated that some requirements concerning the use of network and messaging resources have been provided as part of messaging and network requirements.

4.3.4.2 Capacity

[REQ]

Identifier	REQ-17.01-TS-0260.0005
Title	Maximum size of a message
Requirement	The messaging level infrastructure shall allow the distribution of messages with a size: - up to 2 Mbytes for in-flight downlink and uplink. - up to 20 Mbytes for on-the-ground downlink and uplink.
Status	<validated>
Rationale	Distinct protocols that could satisfy the functional requirements have distinct limitations on the maximum size of a message. Also distinct products offering support for a particular protocol, have specific limits on the maximum size of a message. Limit the maximum message size is also useful to protect against some types of attack. Although the concrete implementation is internal to the SWIM Node, some guidance/suggestions have been identified. Following approach should implemented: - Services are labelled as in-flight or on-the-ground and the labelling applies to concerned messaging resources (e.g. message queue, message topic). - In-flight message queues/topics are configured with 2 MB in the overload protection policy (requirement REQ-17.01-TS-0160.0010). - On-the-flight message queues/topics are configured with 20MB in the overload protection policy. - Overload protection policies for in-flight or on-the-ground are configured with provided limits but they do not prevent to fix different limits. Provided maximum message sizes have been identified by analyzing applicable (Air/Ground SWIM, in-flight, on-the-ground) message samples of digital briefing and AIXM and WXXM.

Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0260.0015
Title	Overall connection limit
Requirement	For the single-ground-swim-node-per-aircraft deployment option, a Ground Purple Profile SWIM Node shall be able to handle up to 4000 concurrent connections.
Status	<validated>
Rationale	The maximum number of concurrent connections on a ground SWIM Node instance can be clearly limited (e.g. hardware appliance) or may allow for (limited) scaling up, (limited) scaling out or a combination of both scaling methods. The required maximum number of concurrent connections, is highly significant for the capacity of finding appropriate solutions. This includes the resources needed to be able to keep information available for the recovery of a connection within the defined applicable time window. Such concurrent connections limit depends on both the deployment option and the stakeholder operating the Ground SWIM Node. The specification does not constrain these options. The provided figure aims at supporting related technical design activities. Furthermore it could be seen as the minimum basis for different deployments.

	The provided figure for single-ground-swim-node-per-aircraft deployment option is based on following considerations: - Ground SWIM Node deployed as part of the Civil AU Operations Centre. - 1000 mainline aircraft (world's largest airline by number of aircraft in its fleet - figure at 2018). - Maximum 4 active concurrent connection per aircraft (Air SWIM Node).
Category	<Performance>
Profile Part	<PP Ground>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0260.0020
Title	Maximum number of concurrent connections per aircraft/Air SWIM Node
Requirement	The Ground Purple Profile SWIM Node shall allow up to 4 concurrent connections per aircraft/Air SWIM Node.
Status	<validated>
Rationale	Needs for all client entities (aircraft and ground systems) with nominal behaviour must be satisfied. Erroneous or misbehaving client entities can jeopardise all shared resources. Concurrent connections limit per client entity depends on several aspects and in

	particular on both the deployment option and Purple Profile enabled SWIM services. The specification does not constrain these options. The provided figure aims at supporting related technical design activities. Furthermore, from the Ground SWIM Node perspective connecting clients could be aircraft and ground-based systems. Taking into account that Air SWIM Node - Ground SWIM Node connections are internal to the SWIM-TI layer, this requirement aims at limiting only these connections. The provided figure is based on following considerations: - for each aircraft 2 downlink connections each for a dedicated Class of Service/priority. - for each aircraft 2 uplink connections each for a dedicated Class of Service/priority. - This represents the full load in a given point in time and it does not mean that all the connections are active gate to gate.
Category	<Performance>
Profile Part	<PP Ground>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0260.0025
Title	Storage for logging
Requirement	Logging functionality shall retain in permanent storage:

	- Non-verbose logs for 30 days. - Verbose logs for 3 days.
Status	<validated>
Rationale	The information to be stored in a logging functionality is expressed in other requirements. Such logging may include information and meta-information on the every attempt to publish or consumer a messages. Distinct product instances may have distinct limitations.
Category	<Performance>
Profile Part	<PP Ground>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0260.0030
Title	Tracing of capacities
Requirement	Trace in relation with capacity requirements shall be put in the log.
Status	<validated>
Rationale	To be able to monitor the resources, traces of identified capacities shall be put in the log.
Category	<Performance>

Profile Part	<PP Ground>
Domain of Interest	<SLA>
Point of View	<SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

4.3.4.3 Time Behaviour

Time behaviour requirements have been defined using the same deployment option characterized for capacity requirements with the load condition described in the table below:

Characteristic	Value
Deployment	"Single" Ground SWIM Node deployment
Maximum number of Air SWIM Nodes connected to the Ground SWIM Node.	1000
Air SWIM Nodes consuming/providing in-flight services	500
Air SWIM Nodes consuming/providing on-the-ground services	500
Maximum number of concurrent connection per Air SWIM Node	4
Air SWIM Node – Ground SWIM Node consolidated maximum concurrent connections	4000
# Of messages per service	10
Average uplink FDRR request messages rate (messages/h) for a given service	5

Average uplink publication messages rate (messages/h) for a given service	5
Consolidated uplink inflight message rate with one service for each PP CoS for each MEPs (messages/h) for all the services	30
Total end to end uplink inflight message rate (messages/h)	15000
Consolidated uplink on-the-ground message rate with one service for each PP CoS for each MEPs (messages/h) for all the services	30
Total end to end uplink on-the-ground message rate (messages/h)	15000
Average downlink FDRR request messages rate (messages/h) for a given service	5
Average downlink publication messages rate (messages/h) for a given service	5
Consolidated downlink inflight message rate with one service for each PP CoS for each MEPs (messages/h) for all the services	30
Total end to end downlink inflight message rate (messages/h)	15000
Consolidated downlink on-the-ground message rate with one service for each PP CoS for each MEPs (messages/h) for all the services	30
Total end to end downlink on-the-ground message rate (messages/h)	15000
Total consolidated uplink and downlink end to end message rate (messages/h)	60000
Observation period (h)	2
Total consolidated uplink and downlink end to end # messages in the observation period	120000

Table 73: Consolidate load characterization for time behaviour requirements

[REQ]

Identifier	REQ-17.01-TS-0230.0010
Title	Messages distribution and routing based on class of services
Requirement	The Air and Ground SWIM Nodes shall be able to handle messages distribution and routing according to class of services.
Status	<validated>
Rationale	ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services performance requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different time behaviour requirements.

	- For a given candidate PP enabled SWIM service, the time behaviour requirements could be different depending on the operational environment (enroute, terminal, airport). The PP is therefore designed to cover heterogeneous time behaviour constraints via class of services. The specification provides a first list of CoSs: additional ones or revised existing CoSs could be added during next phases of the Air/Ground SWIM. The Air SWIM Node has to provide this capability because it could happen that two different services provided/consumed by the A/C have different time behaviour constraints. On the other hand, the Ground SWIM Node has to cover similar needs plus the fact that it may serve more than one A/C each in different operational environment (enroute, terminal, airport) and with different time behaviour constraints. Messages distribution and routing based on class of services is realized by combining PP level ordering guarantees QoSs and network level class of services. Although the concrete implementation is internal to the SWIM Node, some guidance/suggestions have been identified. The implemented solution should be based on composition of class of services at SWIM Node level and class of services at network level. Assigning a CoS to a SWIM service consists in assigning that CoS to concerned messaging resources (e.g. message queue). Two or more CoSs at SWIM Node level may be assigned to the same CoS at network level (this is configurable). In this case the prioritization between the two SWIM Node level CoSs is enforced at SWIM Node level.
Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0230.0015
Title	End to end message latency for CoS Category A
Requirement	End to end message latency for services of Category A shall be as follows: + Measurements: - 95% of the messages <= 20s - 98% of the messages <= 40s + Measurement conditions: - message size <= 2MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 512Kbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.
Status	<in progress>
Rationale	ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services performance requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different time behaviour requirements. - For a given candidate PP enabled SWIM service, the time behaviour requirements could be different depending on the operational environment (enroute, terminal, airport). The PP is therefore designed to cover heterogeneous time behaviour constraints via class of services. The specification provides a first list of CoSs: additional ones or revised existing CoSs could be added during next phases of the Air/Ground SWIM. ED-175 does not provide any information concerning message size, network

	conditions or allocation of times to the different layers. In the context of the PP specification assumptions are made and CoSs time behaviour requirements defined by documenting the measurement conditions. Two competitive constraints have been taken into account: - due to security and capacity needs different maximum message size limits have been identified for in-flight (enroute, terminal) and on-the-ground (airport) information exchange. - the data links available in different environments could provide different bandwidth. For each of identified {max message size, network bandwidth} pairs, two different CoSs have been defined. CoSs for on-the-ground information exchange have a lower priority with respect to CoSs for in-flight information exchange. This requirement concerns the CoS Category A defined taking into account {max message size, network bandwidth} pair identified for in-flight information exchange. This requirement is applicable to both uplink and downlink and to publication, request and response messages (for simplicity the request and response messages have the same size limit). More details and clarifications about the normal load and observation points are provided in the technical specification.
Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0230.0020
Title	End to end message latency for CoS Category B
Requirement	End to end message latency for services of Category B shall be as follows: + Measurements: - 95% of the messages <= 30s - 98% of the messages <= 60s + Measurement conditions: - message size <= 2MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 512Kbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.
Status	<in progress>
Rationale	ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services performance requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different time behaviour requirements. - For a given candidate PP enabled SWIM service, the time behaviour requirements could be different depending on the operational environment (enroute, terminal, airport). The PP is therefore designed to cover heterogeneous time behaviour constraints via class of services. The specification provides a first list of CoSs: additional ones or revised existing CoSs could be added during next phases of the Air/Ground SWIM. ED-175 does not provide any information concerning message size, network conditions or allocation of times to the different layers. In the context of the PP specification assumptions are made and CoSs time behaviour requirements defined by documenting the measurement conditions. Two competitive constraints have been

	taken into account: - due to security and capacity needs different maximum message size limits have been identified for in-flight (enroute, terminal) and on-the-ground (airport) information exchange. - the data links available in different environments could provide different bandwidth. For each of identified {max message size, network bandwidth} pairs, two different CoSs have been defined. CoSs for on-the-ground information exchange have a lower priority with respect to CoSs for in-flight information exchange. This requirement concerns the CoS Category B defined taking into account {max message size, network bandwidth} pair identified for in-flight information exchange. This requirement is applicable to both uplink and downlink and to publication, request and response messages (for simplicity the request and response messages have the same size limit). More details and clarifications about the normal load and observation points are provided in the technical specification.
Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0230.0025
Title	End to end message latency for CoS Category C
Requirement	End to end message latency for services of Category C shall be as follows: + Measurements: - 95% of the messages <= 100s - 98% of the messages <= 150s + Measurement conditions: - message size <= 20MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 2Mbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.
Status	<in progress>
Rationale	ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services performance requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different time behaviour requirements. - For a given candidate PP enabled SWIM service, the time behaviour requirements could be different depending on the operational environment (enroute, terminal, airport). The PP is therefore designed to cover heterogeneous time behaviour constraints via class of services. The specification provides a first list of CoSs: additional ones or revised existing CoSs could be added during next phases of the Air/Ground SWIM. ED-175 does not provide any information concerning message size, network conditions or allocation of times to the different layers. In the context of the PP specification assumptions are made and CoSs time behaviour requirements defined by documenting the measurement conditions. Two competitive constraints have been taken into account:

	- due to security and capacity needs different maximum message size limits have been identified for in-flight (enroute, terminal) and on-the-ground (airport) information exchange. - the data links available in different environments could provide different bandwidth. For each of identified {max message size, network bandwidth} pairs, two different CoSs have been defined. CoSs for on-the-ground information exchange have a lower priority with respect to CoSs for in-flight information exchange. This requirement concerns the CoS Category C defined taking into account {max message size, network bandwidth} pair identified for on-the-ground information exchange. This requirement is applicable to both uplink and downlink and to publication, request and response messages (for simplicity the request and response messages have the same size limit). More details and clarifications about the normal load and observation points are provided in the technical specification.
Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0230.0030
Title	End to end message latency for CoS Category D
Requirement	End to end message latency for services of Category D shall be as follows: + Measurements: - 95% of the messages <= 150s - 98% of the messages <= 200s + Measurement conditions: - message size <= 20MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 2Mbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.
Status	<in progress>
Rationale	ED-175 is used as one possible reference SPR (the solution adopted ED-151 as OSED) for Purple Profile enabled SWIM services performance requirements. The analysis indicates that: - Candidate PP enabled SWIM services have different time behaviour requirements. - For a given candidate PP enabled SWIM service, the time behaviour requirements could be different depending on the operational environment (enroute, terminal, airport). The PP is therefore designed to cover heterogeneous time behaviour constraints via class of services. The specification provides a first list of CoSs: additional ones or revised existing CoSs could be added during next phases of the Air/Ground SWIM. ED-175 does not provide any information concerning message size, network conditions or allocation of times to the different layers. In the context of the PP specification assumptions are made and CoSs time behaviour requirements defined by documenting the measurement conditions. Two competitive constraints have been taken into account:

	- due to security and capacity needs different maximum message size limits have been identified for in-flight (enroute, terminal) and on-the-ground (airport) information exchange. - the data links available in different environments could provide different bandwidth. For each of identified {max message size, network bandwidth} pairs, two different CoSs have been defined. CoSs for on-the-ground information exchange have a lower priority with respect to CoSs for in-flight information exchange. This requirement concerns the CoS Category D defined taking into account {max message size, network bandwidth} pair identified for on-the-ground information exchange. This requirement is applicable to both uplink and downlink and to publication, request and response messages (for simplicity the request and response messages have the same size limit). More details and clarifications about the normal load and observation points are provided in the technical specification.
Category	<Performance>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

4.3.5 Security requirements

This section includes security requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with security NFR sub-characteristics described in ISO/IEC 25010:2011: confidentiality, integrity, non-repudiation, accountability and authenticity. The requirements have been derived from the technical view described in §4.2.2.3.

The consolidated functional view plus technical view security requirements set has to be evaluated taking into account the technical-functional views traceability described in §4.2.2.6.

Furthermore, taking into account that qualities and functions are not the same, the adopted relationships between security functions and ISO/IEC 25010:2011 security sub-characteristic is described in the table below.

	ISO/IEC 25010:2011 Security sub-characteristics				
	Degree to which a product or system ensures that data are accessible only to those authorized to have access.	Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data. It includes immunity ("the degree to which a product or system is resistant to attack").	Degree to which the identity of a subject or resource can be proved to be the one claimed.	Degree to which the actions of an entity can be traced uniquely to the entity.	Degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.
SWIM-TI Security functions and respective realization in the technical view	Confidentiality	Integrity	Authenticity	Accountability	Non-repudiation
Identity Management	No direct relationships with this sub-characteristic. It is an enabler for all the security functions.	No direct relationships with this sub-characteristic. It is an enabler for all the security functions.	Procedures, resources and services for digital identity lifecycle management and revocation status check.	No direct relationships with this sub-characteristic. It is an enabler for all the security functions.	No direct relationships with this sub-characteristic. It is an enabler for all the security functions.
Security Policy management	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Authentication	No direct relationships with this sub-characteristic. It is an enabler for authorization.	No direct relationships with this sub-characteristic. It is an enabler for authorization.	Authentication of the digital identities of subjects offering or consuming messaging resources.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Authorization	Only authorized subjects are allowed to access to messaging resources.	Only authorized subjects are allowed to access to messaging resources.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Audit	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	Audit logging includes identity of the entities accessing or attempting to access messaging resources.	Audit logging includes identity of the entities accessing or attempting to access messaging resources. Audit logs are maintained in secure storage.
Confidentiality ensuring	Transport level/point to point information confidentiality.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Information Integrity and authenticity ensuring	No direct relationships with this sub-characteristic.	Transport level/point to point information integrity.	Transport level/point to point information authenticity.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Message screening	No direct relationships with this sub-characteristic.	Mechanisms protecting immunity of Purple Profile enabled applications.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Overload protection	No direct relationships with this sub-characteristic.	Mechanisms protecting immunity of Purple Profile enabled applications.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Technical view specific requirements	Confidentiality	Integrity	Authenticity	Accountability	Non-repudiation
Message distribution (not included in security REQs set)	It allows to transfer message level security information in a secure and reliable manner.	It allows to transfer message level security information in a secure and reliable manner.	It allows to transfer message level security information in a secure and reliable manner.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Access control to administrative interfaces	RBAC for SWIM Nodes administrative interfaces	RBAC for SWIM Nodes administrative interfaces	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.	No direct relationships with this sub-characteristic.
Clock synchronisation	Transversal	Transversal	Transversal	Transversal	Transversal
Management of technical vulnerabilities (ISO 27002:2013)	Transversal	Transversal	Transversal	Transversal	Transversal

Table 74: Security functions and ISO/IEC 25010:2011 security sub-characteristic

Finally, this specification (functional plus technical views) cover only non-transferred security controls (§4.2.1.1.2).

4.3.5.1 Authenticity

[REQ]

Identifier	REQ-17.01-TS-0110.0080
Title	X.509v3 certificates based authentication
Requirement	X.509 version 3 certificates issued by a CA shall be used as digital identity for system or machine authentication.
Status	<validated>
Rationale	X.509 version 3 certificates is the digital identity type used for authentication. Only certificates issued by a CA are allowed: self-signed certificates are not allowed). This requirement covers NIST security controls IA-5 c, IA-5 (2) a and IA-3.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0325

[REQ]

Identifier	REQ-17.01-TS-0270.0200
Title	Amqps form for mutual transport level authentication of AMQP 1.0 peers
Requirement	AMQP 1.0 peers shall be mutual authenticated through TLS and in accordance with the amqps form.

Status	<validated>
Rationale	The Purple Profile is in charge of ensuring point-to-point security via transport level security mechanisms. Transport level security applies to all the directly connected messaging entities in the messaging technical view: access to message queues, message topics and subscription handlers is mutual authenticated, authorized and protected in terms of confidentiality and integrity The adopted transport level security mechanism is IANA amqps as defined in the AMQP 1.0 §5.2.1. Although in Purple Profile the mutual authentication is at amqps level, it should be noted that some available AMQP libraries/OTSs requires the use of SASL anonymous when using amqps.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0300
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0305
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0310
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0315
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0320

[REQ]

Identifier	REQ-17.01-TS-0440.0040
Title	TLS1.2 RFC 5246 interoperability standard
Requirement	IETF RFC 5246 TLS 1.2 shall be used for transport level security.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008, http://tools.ietf.org/html/rfc5246, is used as transport level security mechanism. Both TLS 1.2 and TLS 1.3 are allowed. This requirement covers NIST security controls SC-13.
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0041
Title	TLS1.3 RFC 8446 interoperability standard

Requirement	IETF RFC 8446 TLS 1.3 shall be used for transport level security.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. IETF RFC 8446, "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018, https://www.rfc-editor.org/rfc/rfc8446.txt, is used as transport level security mechanism. Both TLS 1.2 and TLS 1.3 are allowed. This requirement covers NIST security controls SC-13.
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0205
Title	Prohibited fallback to any TLS or SSL version lower than TLS 1.2
Requirement	Fallback to any TLS or SSL version lower than TLS 1.2 shall be prohibited.
Status	<validated>
Rationale	For security reasons fallback to TLS or SSL version lower than TLS 1.2 is prohibited. This is also in accordance with IETF RFC 7568 (Deprecating Secure Sockets Layer

	Version 3.0), IETF RFC 6176 (Prohibiting Secure Sockets Layer (SSL) Version 2.0) and NIST SP800-52 revision 1 and draft revision 2.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0210
Title	Allowed fallback from TLS 1.3 to TLS 1.2
Requirement	Fallback from TLS 1.3 to TLS 1.2 shall be allowed.
Status	<validated>
Rationale	For security reasons only the fallback to TLS 1.2 is allowed. Additional restrictions of both TLS 1.2 and 1.3 concern the allowed/recommended cipher suites and TLS extensions. These are typically provided as part of domain-specific regulations.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0215
Title	X.509v3 revocation status check
Requirement	The Amqps peer shall perform revocation checking of the remote Amqps peer's X.509v3 certificate.
Status	<validated>
Rationale	X.509v3 certificate revocation status check is mandatory. Each Amqps peer (i.e. AMQP 1.0 over TLS in the amqps form) involved in the mutual authentication has to check the revocation status of the remote peer's X.509v3 certificate.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0220
Title	X.509v3 revocation status check based on locally stored CRL
Requirement	The X.509v3 certificate revocation status shall be obtained from Certificate Revocation List (CRL) in the local store.
Status	<validated>
Rationale	The X.509v3 certificate revocation check is usually performed by: - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or - Consuming OCSP (Online Certificate Status Protocol) service(s), or - Combining both CRL and OCSP based certification revocation status mechanisms. In the Purple Profile the basic (<PP Core>) option for checking X.509 certificate revocation status is to rely on locally stored CRLs. The capability of Purple Profile enabled applications and SWIM Nodes to use OCSP based revocation status check is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts).
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0225
Title	Schedule CRLs maintenance
Requirement	Maintenance process shall be scheduled ensuring that CRLs are updated before they expire.
Status	<in progress>
Rationale	The CRL is one and the basic option for obtaining the revocation status information for X.509v3 certificates. The CRLs expire (they are signed and they can only be trusted for a limited time): an expired CRL represents a possible vulnerability (e.g. certificates could be revoked in the meantime). Fresh CRLs are retrieved via CRL distribution point (CDP). CAs typically provide online CDPs over HTTP and/or over LDAP (LDAP CDP) and the endpoint addresses of these services could be also included in the certificates they issue). CDPs could be consumed: - as part of scheduled maintenance activities, or - on-the-fly during the authentication. Basic (<PP Core>) Purple Profile option is based on a scheduled maintenance process ensuring that CRL are updated before they expire. The capability of Purple Profile enabled applications and SWIM Nodes to use HTTP CDPs and/or LDAP CDPs is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts).
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0230
Title	Successful mutual authentication requires valid X.509v3 certificates
Requirement	In case the peer's X.509v3 certificate is revoked or expired, the TLS session establishment shall be interrupted reporting the peer with applicable TLS error alert.
Status	<validated>
Rationale	Is it possible that one or both peers continue the TLS session establishment also in case one of the certificates is expired or revoked. This requirement introduces constraints on possible behaviour of the peers in case the X.509v3 certificate is expired or revoked. There are additional TLS errors alerts concerning the authentication (e.g. "unknown_ca"). Certificate profile and CAs trust should be properly evaluated in order to minimize the impact of the authentication.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0235
Title	Authentication in case of not current or inappropriate CRL
Requirement	When the local CRL is not the current CRL or the CRL scope is not appropriate for the certificate in question, the peer shall either reject the certificate or accept a potentially revoked or compromised certificate depending on its Authentication policy.
Status	<in progress>
Rationale	At the time of the authentication, the local CRL could be not the current CRL (CRL expiration, next update, etc.) or the CRL scope could be not appropriate (RFC 5280). Taking into account that In the <PP Core> the CDPs are not mandated, by definition it is not possible to refresh/download a proper CRL. In this situation the decision to accept or reject the certificate, is defined in the peer's authentication policy.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0240
Title	Delta-CRL support
Requirement	The CRLs update mechanisms shall be able to handled delta-CRL.
Status	<in progress>
Rationale	CRLs size can get potentially significantly large over the time by affecting bandwidth consumption and processing time. These effects become more relevant as the CRL publication frequency is increased. In order to meet performance requirements, CA provides Delta CRL policy to properly manage both Delta and Base CRL size to limit network bandwidth. Delta CRLs, allowing relying party to download the large CRL less frequently and the Delta more frequently. Basic (<PP Core>) Purple Profile option is that, as relying party, only the capabilities to handle base-CRL are required. Advanced Purple Profile enabled applications and SWIM Nodes conformant to <PP Air Security+> or <PP Ground Security+> profile parts have to be able to handle delta-CRLs.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0245
Title	CRL partitioning support
Requirement	The CRLs update mechanisms shall be able to handled CRL partitioning.
Status	<in progress>
Rationale	CRLs size can get potentially significantly large over the time by affecting bandwidth consumption and processing time. These effects become more relevant as the CRL publication frequency is increased. CRL partitioning is a mechanism typically provided by CAs to cover some cases including (but not limited to) large CRLs. Advanced Purple Profile enabled applications and SWIM Nodes (relying parties) conformant to <PP Air Security+> or <PP Ground Security+> profile parts have to be able to handle CRL partitioning.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0250
Title	On-the-fly CRL update
Requirement	The CRL distribution points (CDPs) shall be used to update CRLs on-the-fly.
Status	<validated>
Rationale	The CRL is one and the basic option for obtaining the revocation status information for X.509v3 certificates. The CRLs expire (they are signed and they can only be trusted for a limited time): an expired CRL represents a possible vulnerability (e.g. certificates could be revoked in the meantime). Fresh CRLs are retrieved via CRL distribution point (CDP). CAs typically provide online CDPs over HTTP and/or over LDAP (LDAP CDP) and the endpoint addresses of these services could be also included in the certificates they issue). CDPs could be consumed: - as part of scheduled maintenance activities, or - on-the-fly during the authentication. The capability of Purple Profile enabled applications and SWIM Nodes to use HTTP CDPs and/or LDAP CDPs is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts). This requirement aims at allowing CRLs to be updated automatically when required and in-between scheduled maintenance activities. On-the-fly CRL update introduces delay in the overall authentication process. A possible solution limiting the delay is to demand to a dedicated process/thread the automatic, periodic and scheduled check & update of the CRL: this reduces the probability of the occurrence of on the fly CRL update during the authentication process. This specification provides standard based interface bindings to access CDPs. The bindings are typically exposed by CAs and the Purple Profile entities consume them.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0800.0115
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0800.0110

[REQ]

Identifier	REQ-17.01-TS-0270.0255
Title	CDPs URLs from peer's certificate
Requirement	The CRLs update mechanisms shall be able to use the CRL Distribution Points in the CDPs extension in the peer's certificate.
Status	<validated>
Rationale	Depending on the X.509v3 certificate profile, the CDPs extension may be available in the peer's certificate. This requirement allows to use as CDPs URLs the information included in this extension.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0330

[REQ]

Identifier	REQ-17.01-TS-0270.0260
Title	X.509v3 revocation status check based on OCSP
Requirement	The X.509v3 certificate revocation status shall be obtained from OCSP response from OCSP responder.
Status	<validated>
Rationale	The X.509v3 certificate revocation check is usually performed by: - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or - Consuming OCSP (Online Certificate Status Protocol) service(s), or - Combining both CRL and OCSP based certification revocation status mechanisms. The capability of Purple Profile enabled applications and SWIM Nodes to use OCSP based revocation status check is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts). This specification provides standard based interface binding to access OCSP service. The binding is typically exposed by CAs and the Purple Profile entities consume it.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0800.0105

[REQ]

Identifier	REQ-17.01-TS-0270.0265
Title	OCSP responder URLs from local configuration
Requirement	The OCSP requestor shall be able to obtain the OCSP responder URL(s) from pre-configured local resources.
Status	<validated>
Rationale	Depending on the X.509v3 certificate profile, the Authority Information Access extension may be available or not in the peer's certificate. In case the extension is not used or additional OCSP responder URLs are required, this information can be retrieved from local resources.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0270
Title	OCSP responder URLs from peer's certificate
Requirement	The OCSP requestor shall be able to obtain the OCSP responder URL(s) from the location identified in the OCSP field in the Authority Information Access extension in the peer's certificate.
Status	<validated>
Rationale	Depending on the X.509v3 certificate profile, the Authority Information Access extension may be available in the peer's certificate. This requirement allows to use as OCSP responder URLs the information included in this extension.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0275
Title	OCSP responses caching
Requirement	The OCSP requestor should implement OCSP responses caching.
Status	<validated>
Rationale	A possible mechanism that could be used on the OCSP requestor side to reduce the performance overhead due to on-line revocation status check, is to implement OCSP responses caching: responses are cached and, when possible and still valid, reused to obtain the revocation status of a certificate without submitting a request to the OCSP responder. However, it could happen that there is no cached response for that certificate: in this case a request is sent to the OCSP responder and the response cached on the requestor side. OCSP responses caching is typically implemented by relying on timestamping information: responses have a TTL that could be defined on the requestor side or evaluated according to times included in the OCSP response. The OCSP standard includes mechanisms a responder may use to provide the requestor with times information about the response. In particular the responses can contain three times (thisUpdate, nextUpdate and producedAt) that a requestor may use to implement OCSP responses caching (e.g. nextUpdate indicate when the newer information will be available - this represents the response TTL).
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0300
Title	OSCP response max size
Requirement	OSCP response shall not exceed a defined maximum size.
Status	<in progress>
Rationale	For the swim environment, the OSCP responses must not exceed the maximum size supported by the system. If a response is larger than the maximum size allowed, the response is ignored and treated the same as a response that indicates unknown certificate status. This maximum size shall be defined according to system memory size. For example: IBM OSCP maximum response size is by default configured to 20480 bytes.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0305
Title	OSCP secure providers
Requirement	OSCP providers shall be secure and authorized.
Status	<in progress>
Rationale	OCSP providers are expected to be secure (certified, EU/ICAO regulations, ATM regulations) and communications with authorized responders must be ensured according to RFC2560, 4.2.2.2.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0310
Title	OCSP replay attacks
Requirement	OCSP requestor shall be protected against OSCP replay attacks.
Status	<in progress>
Rationale	There is a possibility that an out of date OCSP response could be replayed, thus causing a client to accept a good response when in fact there is a more up-to-date response that specifies the status of revoked certificate. To mitigate this attack, the OCSP requestor (SWIM TI or application level entity) must check the freshness of

	OSCP responses according to a reliable source of time.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0315
Title	OCSP Man-in-the-middle attacks
Requirement	OCSP requestor shall be protected against OCSP Man-in-the-middle attacks.
Status	<in progress>
Rationale	OCSP requestor (SWIM TI or application level entity) must properly validate the signature on the OCSP response. The use of signed responses in OCSP serves to authenticate the identity of the OCSP responder and to verify that it is authorized to sign responses on the CA's behalf. System must ensure that it is communicating with an authorized responder.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0280
Title	Combined OCSP and CRL based revocation status check
Requirement	Combined OCSP and CRL based X.509v3 certificate revocation status check mechanism shall be provided.
Status	<validated>
Rationale	Advanced Purple Profile enabled applications and SWIM Nodes conformant to <PP Air Security+> or <PP Ground Security+> profile parts rely on X.509v3 certificate revocation status check solutions allowing to combine both OCSP and CRL based mechanisms.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0330

[REQ]

Identifier	REQ-17.01-TS-0270.0285
Title	Composition options for combined OCSP and CRL based revocation status check
Requirement	Combined OCSP and CRL based X.509v3 certificate revocation status check mechanism shall allow to configure following options: - OCSP preferred and, when the fallback is enabled, CRL as fallback. - CRL preferred and, when the fallback is enabled, OCSP as fallback.
Status	<validated>
Rationale	This requirement provides the OCSP-CRL composition options.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0290
Title	Fallback enabling/disabling for combined OCSP and CRL based revocation status check
Requirement	Combined OCSP and CRL based X.509v3 certificate revocation status check mechanism shall allow to disable and enabled OCSP-CRL / CRL-OCSP fallback.
Status	<validated>
Rationale	The identified composition options for combined OCSP and CRL based revocation status check depend on the possibility to enabled/disable OCSP-CRL and CRL-OCSP fallback.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0295
Title	Authentication in case of not current or inappropriate CRL and unavailable or inaccessible OCSP responder and/or CDP
Requirement	When - the local CRL is not the current CRL, or - the CRL scope is not appropriate for the certificate in question, or - no valid OCSP response is available locally, and the OCSP responder or/and the CDP are unavailable or inaccessible, the peer shall either reject the certificate or accept a potentially revoked or compromised certificate depending on its Authentication policy.
Status	<validated>
Rationale	Irrespective of the option used to combine OCSP and CRL based revocation status check, following events may occur at the time of authentication (TLS session establishment): - the local CRL could be not the current CRL (CRL expiration, next update, etc.) or the CRL scope could be not appropriate (RFC 5280): in this case the appropriate/updated CRL should be retrieved via the CDP. - when implementing OCSP responses caching, not locally cached responses could be used (because response TTL or because no response about the certificate in question have been cached): in this case a new request has to be sent to the OCSP responder. OCSP responder and CDP are accessible over the network: it could happen that they are not available or reachable. In this situation the decision to accept or reject the certificate, is defined in the peer's authentication policy.
Category	<Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authentication Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0335

4.3.5.2 Confidentiality

[REQ]

Identifier	REQ-17.01-TS-0280.0010
Title	AMQP 1.0 peers transport level confidentiality
Requirement	Confidentiality of the information exchanged between AMQP 1.0 peers shall be protected through TLS.
Status	<validated>
Rationale	TLS {1.2|1.3} provides point to point transport level security (including confidentiality) between AMQP 1.0 peers. Transport level confidentiality is provided via connection specific symmetric key or AEAD in TLS 1.2 or AEAD in TLS 1.3.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Confidentiality Ensuring Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0130.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0010
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0015
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0020
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0025
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0030
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0165
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0170
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0175

[REQ]

Identifier	REQ-17.01-TS-0280.0015
Title	Message level confidentiality information transfer for security information detached from the data
Requirement	The SWIM-TI Message distribution over AMQP 1.0 shall allow to transfer message level confidentiality information detached from the data in the following form: - content-type AMQP Bare Message Standard property: “application/octet-stream”. - AMQP Bare message application-data section: one data section or a single amqp-value section containing encrypted data. - AMQP footer <key,value> pair: key=ENPT. value=semicolon separated Encryption-Algorithm and Encryption-Secret.
Status	<validated>
Rationale	The Purple Profile provides two mechanisms to transfer message level security information from the sender to the intended recipient(s): - Security information attached to the data: the application-data section within the AMQP bare message includes both data and security information (e.g. digital signature). Examples of applicable standards are S/MIME 3.2, XML signature and XML encryption. - Security information detached from the data: the application-data section within the AMQP bare message includes plain or encrypted data and cryptographic information

	(message digest, digital signature, etc.) are included in the AMQP 1.0 footer section. This requirement concerns the message level confidentiality information transfer for security information detached from the data. The AMQP 1.0 core standard requires that a registry of defined footers and their meanings is maintained but at the time of writing this specification (December 2018) no footers have been registered. This is why the Purple Profile provides the syntax and semantics for using the footer to transfer such message level security information. Symmetric Encryption algorithm identifier should be in accordance with RFC 3370. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations Encryption-Secret is an optional field containing one or more comma separated “uuid” and “secret” pairs. For each intended recipient a colon separated “uuid” and “secret” pair is provided. The uuid is the name-based UUID of the recipient and the “secret” is the symmetric key encrypted with the recipient’s public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The “uuid” and “secret” pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e. publication messages) a mechanism should be put in place in order to allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid” and “secret” pairs in accordance with active subscribers’ UUIDs. Taking into account the potential number of recipients, the full set of “uuid” and “secret” pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0040
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0130.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0035
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0190

4.3.5.3 Integrity

[REQ]

Identifier	REQ-17.01-TS-0290.0010
Title	AMQP 1.0 peers transport level Integrity and authenticity
Requirement	Integrity and authenticity of the information exchanged between AMQP 1.0 peers shall be protected through TLS.
Status	<validated>
Rationale	TLS {1.2|1.3} provides point to point transport level security (including integrity and authenticity) between AMQP 1.0 peers. Transport level integrity and authenticity is provided via HMAC or AEAD in TLS 1.2 or AEAD in TLS 1.3.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Information Integrity And Authenticity Ensuring Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0140.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0010
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0015
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0020
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0025
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0030
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0200
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0110.0205

[REQ]

Identifier	REQ-17.01-TS-0290.0015
Title	HMAC based Message level Integrity and authenticity information transfer for security information detached from the data
Requirement	The SWIM-TI Message distribution over AMQP 1.0 shall allow to transfer message level integrity and authenticity information detached from the data in the following form: - content-type AMQP Bare Message Standard property: Not restricted. - AMQP Bare message application-data section: one data section or a single amqp-value section. - AMQP footer <key,value> pair: key=HMAC. value=semicolon separated HMAC-Algorithm, HMAC-Target, HMAC-Digest and HMAC-Secret.
Status	<validated>
Rationale	The Purple Profile provides two mechanisms to transfer message level security information from the sender to the intended recipient(s): - Security information attached to the data: the application-data section within the AMQP bare message includes both data and security information (e.g. digital

	signature). Examples of applicable standards are S/MIME 3.2, XML signature and XML encryption. - Security information detached from the data: the application-data section within the AMQP bare message includes plain or encrypted data and cryptographic information (message digest, digital signature, etc.) are included in the AMQP 1.0 footer section. This requirement concerns the HMAC based message level integrity and authenticity information transfer for security information detached from the data. The AMQP 1.0 core standard requires that a registry of defined footers and their meanings is maintained but at the time of writing this specification (December 2018) no footers have been registered. This is why the Purple Profile provides the syntax and semantics for using the footer to transfer such message level security information. HMAC-Algorithm: HMAC cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations HMAC-Target: {bare, data}. It indicates if the HMAC is calculated on the entire AMQP bare message ("bare") or only on the application-data section ("data"). HMAC-Digest: Base64 encoded message digest. HMAC-Secret: optional field containing one or more comma separated "uuid" and "secret" pairs. For each intended recipient a colon separated "uuid" and "secret" pair is provided. The uuid is the name-based UUID of the recipient and the "secret" is the symmetric key encrypted with the recipient's public key and base64 encoded. The selected asymmetric encryption algorithm must be documented and it must comply with applicable security policies, best practices and regulations. The "uuid" and "secret" pairs are calculated/recalculated only when new recipient is added and/or the secret key renewed. For one/many to many information exchange (i.e. publication messages) a mechanism should be put in place in order to allow the publisher and the subscription handler to share the same view about active subscribers: this allows the publisher to properly manage the uuid" and "secret" pairs in accordance with active subscribers' UUIDs. Taking into account the potential number of recipients, the full set of "uuid" and "secret" pairs is not mandated to be sent for each message. The full set could be sent periodically and intermediate messages could include only pairs concerning added recipients. In case the (uuid, secret) pair mechanism is not used, the way the shared secret is exchanged/generated/renewed shall be documented as part of the SWIM service design specification.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0040
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0035
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0190

[REQ]

Identifier	REQ-17.01-TS-0290.0020
Title	Digital Signature based Message level Integrity and authenticity information transfer for security information detached from the data
Requirement	The SWIM-TI Message distribution over AMQP 1.0 shall allow to transfer message level integrity and authenticity information detached from the data in the following form: - content-type AMQP Bare Message Standard property: Not restricted. - AMQP Bare message application-data section: one data section or a single amqp-value section. - AMQP footer <key,value> pair: key=DSGN. value=semicolon separated DSGN-Algorithm, DSGN-Target and DSGN-Signature.
Status	<validated>
Rationale	The Purple Profile provides two mechanisms to transfer message level security information from the sender to the intended recipient(s):

	- Security information attached to the data: the application-data section within the AMQP bare message includes both data and security information (e.g. digital signature). Examples of applicable standards are S/MIME 3.2, XML signature and XML encryption. - Security information detached from the data: the application-data section within the AMQP bare message includes plain or encrypted data and cryptographic information (message digest, digital signature, etc.) are included in the AMQP 1.0 footer section. This requirement concerns the Digital Signature based message level integrity and authenticity information transfer for security information detached from the data. The AMQP 1.0 core standard requires that a registry of defined footers and their meanings is maintained but at the time of writing this specification (December 2018) no footers have been registered. This is why the Purple Profile provides the syntax and semantics for using the footer to transfer such message level security information. DSGN-Algorithm: Digital signature cryptographic algorithm identifier. Identifiers should be in accordance with RFC 3370, RFC 5754 and RFC 4231. Different conventions should be documented. The selected algorithm must comply with applicable security policies, best practices and regulations. DSGN-Target: {bare, data}. It indicates if the digital signature is calculated on the entire AMQP bare message (“bare”) or only on the application-data section (“data”). DSGN-Signature: Base64 encoded digital signature. On the receiver side, the lookup of sender’s public key to be used for digital signature validation relies on the user-id property (e.g. the alias used in the keystore could be the name-based uuid).
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0040
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0140.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0035
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0190

[REQ]

Identifier	REQ-17.01-TS-0290.0025
Title	Senders authorization based on authenticated digital identity (i.e. X.509v3 certificate)
Requirement	The AMQP peer's digital identity authenticated at transport level shall be used to authorize senders to send messages to a message queue.
Status	<validated>
Rationale	Only authorized entities are allowed to access message queues. The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers). This requirement covers NIST security controls AC-3 and AC-24.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Authorization Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0120.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0120.0010

[REQ]

Identifier	REQ-17.01-TS-0290.0030
Title	Receiver authorization based on authenticated digital identity (i.e. X.509v3 certificate)
Requirement	The AMQP peer's digital identity authenticated at transport level shall be used to authorize receiver to consume messages from a message queue.
Status	<validated>
Rationale	Only authorized entities are allowed to access message queues. The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers). This requirement covers NIST security controls AC-3 and AC-24.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0120.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0120.0015

[REQ]

Identifier	REQ-17.01-TS-0290.0035
Title	Publishers authorization based on authenticated digital identity (i.e. X.509v3 certificate)
Requirement	The AMQP peer's digital identity authenticated at transport level shall be used to authorize publishers to publish messages to a message topic.
Status	<validated>
Rationale	Only authorized entities are allowed to access message topics. The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers). This requirement covers NIST security controls AC-3 and AC-24.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Publisher><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0120.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0120.0020

[REQ]

Identifier	REQ-17.01-TS-0290.0040
Title	Subscribers authorization based on authenticated digital identity (i.e. X.509v3 certificate)
Requirement	The AMQP peer's digital identity authenticated at transport level shall be used to authorize subscribers to consume messages from a message topic.
Status	<validated>
Rationale	Only authorized entities are allowed to access message topics. The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers). This requirement covers NIST security controls AC-3 and AC-24.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0120.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0120.0025

[REQ]

Identifier	REQ-17.01-TS-0290.0045
Title	Subscription authorization based on authenticated digital identity (i.e. X.509v3

	certificate)
Requirement	The AMQP peer's digital identity authenticated at transport level shall be used to authorize subscribers to send subscription management messages to a subscription handler.
Status	<validated>
Rationale	Only authorized entities are allowed to interact with the subscription handlers. The digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources (queues, topics, subscription handlers). This requirement covers NIST security controls AC-3 and AC-24.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<Function/Behaviour>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Authorization Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0120.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0120.0030

[REQ]

Identifier	REQ-17.01-TS-0270.0025
Title	SWIM Security Application Message Integrity Ensuring

Requirement	Application level messages integrity shall not be violated during any processing at SWIM-TI level.
Status	<validated>
Rationale	The SWIM-TI Security shall maintain the integrity of the user messages when performing security enforcement.
Category	<Security><Design>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0095
Title	Protection of configuration
Requirement	SWIM node configuration (policy, routing tables) shall be protected from unauthorized access.
Status	<validated>
Rationale	To protect configuration from unauthorized access.
Category	<Security>
Profile Part	<PP Core>

Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0320
Title	Protection of configuration files' integrity
Requirement	Configuration files' integrity must be ensured.
Status	<in progress>
Rationale	SWIM Node's configuration files should be hashed for an integrity control purpose. A lightweight integrity control application shall be included in the system supporting SWIM communications. The purpose of this application is to generate hashes of the configuration files after each configuration modification and store them in its database. Their integrity shall be ensured by appropriates security measures at application and system level.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0325
Title	Alerting in case of loss of configuration files integrity
Requirement	Alerts shall be emitted in case of unwanted configuration files modifications.
Status	<in progress>
Rationale	Procedures shall include the checking of configuration files at maintenance time, using a lightweight application dedicated to this purpose. Maintenance responsible shall alert in case of loss of configuration files integrity.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0330
Title	Monitoring configuration files
Requirement	Configuration files integrity shall be monitored at maintenance time.
Status	<in progress>
Rationale	Configuration files should be monitored at maintenance times, using a lightweight application dedicated to this purpose.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0050
Title	Partitioning of functionalities
Requirement	Access control to SWIM-TI management functionalities shall be granted leveraging on Role based access control (RBAC) mechanisms.
Status	<validated>

Rationale	Management functionalities include, for example, functions necessary to administer databases, network components, workstations, or servers typically require privileged user access .In order to allow access only to authorized users, SWIM-TI shall use an RBAC model to gain access to management functionalities. This requirement covers NIST security control SC-2.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0335
Title	Administration accounts
Requirement	Administration accounts shall be personal.
Status	<in progress>
Rationale	Each configuration actions must be traced at application and system levels. For that purpose, maintenance and administration account must be personal. Maintainers shall provide their staff personal accounts and security policies, which specify password secrecy rules. Staff must be sensibiliser to the protection of their personal credentials.
Category	<Security>

Profile Part	<PP Core>
Domain of Interest	<ICD><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0055
Title	Security function isolation
Requirement	Access control to SWIM-TI security functionalities shall be implemented according to least privilege principle and leveraging on RBAC mechanisms.
Status	<validated>
Rationale	This requirement is necessary to protect the integrity of security related functionalities of SWIM-TI. Security functionalities include, for example, functions necessary to configure PKI services, administer Identity Store and define and enforce Security Policies. These functionalities typically require privileged user access. This requirement covers NIST Security Control SC-3.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><Governance>
Point of View	<SWIM-TI provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0080
Title	Security protection based on "positive" model
Requirement	Security shall be protected using the "positive" model also known as "whitelist".
Status	<validated>
Rationale	Common practice. The "positive" model can be considered to define what is allowed and reject everything else.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

4.3.5.4 Accountability

[REQ]

Identifier	REQ-17.01-TS-0270.0065
Title	Security functions execution evidence
Requirement	Evidence of the correct execution of security functions shall be provided in the form of either an acknowledgement or auditing.
Status	<in progress>
Rationale	This requirement ensures the SWIM-TI Security has the capability to verify that security functions have not been tampered and thus are being executed properly and to perform this check on certain transitions on demand or with certain defined periodicity. This requirement covers the following NIST security controls: SI-6.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0070
Title	Safe storage for audit logs
Requirement	SWIM-TI audit logs shall be stored in a secure storage.
Status	<in progress>
Rationale	Audit logs includes all information needed to successfully audit information system activity, therefore audit logs and audit tools shall be protected from unauthorized access, modification, and deletion. This should be achieved applying both logical and physical protection of audit logs. Logical protection can be addressed by enforcing adequate Security Policies to grant access to audit logs, while physical protection is addressed by media protection controls and physical and environmental protection controls. This requirement covers NIST security control AU-9.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0075
Title	Remote and independent storage for audit logs
Requirement	SWIM-TI audit data shall be stored in a storage location remote and independent from the system generating the audit data.
Status	<in progress>
Rationale	Audit logs need to be stored in an independent and remote system. This requirement helps to ensure that a compromise of a system being part of SWIM-TI does not also result in a compromise of the corresponding audit records. This requirement covers NIST security control AU-9 (2).
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Function>	Audit Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0340

Title	Security auditing
Requirement	Security logs shall be audited.
Status	<in progress>
Rationale	Audit logs shall be manually or automatically audited. Goals of auditing is to assess accesses, actions on the system, time of actions and their consistency. Auditing shall be formalised under detection rules used in a local or centralized system whose purpose is to emit alerts in case of unwanted connections attempts and unexpected comportments. In case of a centralized system, logs content should be sent using adequate protection to a collection deposit system. In case of local detection, engine should be host-based. Detection rules shall be conceived on the base the system's risk analysis to be as complete as possible.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0345
Title	Security alerts
Requirement	Security auditing shall emit alerts.
Status	<in progress>
Rationale	Auditing shall emit alerts to competent people whom shall take actions regarding to

	risks system faces.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<Function/Behaviour>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

4.3.5.5 Non-repudiation

Requirements concerning this sub-characteristic have not been identified during SESAR 2020 programme. This sub-characteristic should be further investigated according to the evolution of this technical specification (e.g. industrialization, deployment, standardization, etc.). It is however anticipated that some requirements concerning audit logging have been provided as part of security requirements in the functional viewpoint (§4.3.1.2).

4.3.5.6 Crosscutting

[REQ]

Identifier	REQ-17.01-TS-0270.0035
Title	Cryptographic algorithms and key sizes NIST 800-131A compliance
Requirement	Cryptographic algorithms and key sizes shall comply with NIST 800-131A Revision 1 recommendations.
Status	<validated>
Rationale	NIST Special Publication 800-131A 'Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" recommendations represent a

	reference that is used to analyse and to identify the most appropriate cryptographic algorithms and key sizes. The NIST SP 800-131A recommendations must be considered as a minimum set of constraints which may be further restricted in specific policies and/or governance bodies. This requirement covers NIST security controls IA-5c, IA-7 and SC-13.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0190
Title	Cryptographic algorithms FIPS 140-2 Annex A compliance
Requirement	Cryptographic algorithms shall comply with security requirements for cryptographic modules described in the FIPS 140-2 Annex A (approved security functions).
Status	<validated>
Rationale	FIPS 140-2 provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of cryptographic modules. This requirement concerns only the approved security functions described in the FIPS

	140-2 Annex A. This complements recommendations from NIST SP 800-131A. These recommendations must be considered as a minimum set of constraints which may be further restricted in specific policies and/or governance bodies. For instance, recommended cipher suites for TLS may be identified starting from the draft NIST Special Publication 800-52 revision 2 (guidelines for the selection, configuration, and use of TLS implementations).
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0350
Title	Encryption keys length
Requirement	Encryption keys length shall be at the state of art.
Status	<in progress>
Rationale	Encryption keys lengths should be in accordance with latest approved regulations/recommendations. Only the minimum key length approved and, possibly, larger lengths, compliant with encryption algorithm, shall be accepted.
Category	<Security>
Profile Part	<PP Core>

Domain of Interest	<ICD><SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0020
Title	Network connection Shutdown
Requirement	Network connections, associated with a communication session, shall be terminated at the end of the session or after a policy defined the amount of time, to prevent unauthorized access to the system.
Status	<validated>
Rationale	Unneeded network connections are potential security breaches as they may be used by unauthorized bystanders. Terminations of such connections minimizes this risk, e.g. when maintenance operations are on-going. This requirement covers NIST security control SC-1.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0040
Title	Built-in security mechanisms for technology vulnerabilities handling
Requirement	Software components shall be kept up-to-date in terms of security patches concerning the known technology vulnerabilities listed in available vulnerability reporting frameworks.
Status	<validated>
Rationale	This is a common security practice. Software components have to be kept up-to-date in terms of security patches. The longer a known vulnerability remains unpatched, the higher the risk for exploit. It will be desirable to apply security patches within 3 months after publication of the security patch. Several vulnerability databases exist (e.g. NVD, or MITRE CVE).Security control source: Technology Specific Vulnerabilities.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0045
Title	Protection of running systems during and after power outage
Requirement	During or after power outage, security of running systems shall be protected.
Status	<in progress>
Rationale	This requirement implies that security capabilities shall start first and stop last.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<ICD><SLA>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0270.0105
Title	No Air SWIM Node TCP/UDP ports for ground initiated connections
Requirement	The Air SWIM node shall not listen on any (UDP, TCP) port for ground initiated connections.
Status	<validated>
Rationale	In order to avoid TCP server attacks, the Air SWIM Node will strictly act as a TCP client in the communication with the ground SWIM Node, meaning only aircraft-initiated connections are allowed.
Category	<Security>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0450.0005
Title	Time synchronization at SWIM-TI and application layers
Requirement	SWIM Nodes and SWIM enabled applications shall have time synchronized to Coordinated Universal Time (UTC) time zone with an accuracy of 1 second.
Status	<validated>

Rationale	Time synchronization is a must to have for all the security functions and also for reliability purposes. For instance, security and identity tokens are checked for freshness in order to ensure that they are still within their valid lifetimes. Another security related example where time synchronization is needed is exchanging of audit information. The time synchronization is important across a distributed environment and not only for security purpose. The Purple Profile does not constrain how the time is synchronized but how good the time has to be synchronized. This requirement covers NIST security control AU-8.
Category	<Security>
Profile Part	<PP Core>
Domain of Interest	<SLA>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0130
Title	Interoperability standard DNSSec
Requirement	IETF RFC 4033 Domain Name System Security Extensions (DNSSEC) shall be used for DNS based names resolution.
Status	<in progress>

Rationale	Local (LAN), enterprise level and public Domain Name Systems (DNSs) may be used for names resolution when addressing specific networked resource (message queue, OCSP, etc.). This may introduce vulnerabilities that are mitigated via the advanced and optional use of Domain Name System Security (DNSSEC): it extends the DNS standard by providing the resolvers with origin authentication and integrity of DNS data. The standard is defined in the IETF RFC 4033, March 2005 https://tools.ietf.org/html/rfc4033. This requirement covers NIST security control SC-21.
Category	<Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0320.0010
Title	Air Purple Profile SWIM Node X.509 Certificate
Requirement	On board usage of Air Purple Profile SWIM Node certificate shall follow ARINC 842-2 GUIDANCE FOR USAGE OF DIGITAL CERTIFICATES.
Status	<validated>
Rationale	According to Arinc 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK recommendations.

Category	<Security>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0320.0015
Title	Air Purple Profile SWIM Node Security events logging
Requirement	On board logging of AIR SWIM TI security event shall follow ARINC 852 GUIDANCE FOR SECURITY EVENT LOGGING IN AN IP ENVIRONMENT.
Status	<validated>
Rationale	According to Arinc 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK recommendations.
Category	<Security>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0320.0020
Title	Air Purple Profile SWIM Node KEY MANAGEMENT
Requirement	On board logging of AIR SWIM TI security event shall follow A823 DATALINK SECURITY PART 2 – KEY MANAGEMENT.
Status	<validated>
Rationale	According to Arinc 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK recommendations.
Category	<Security>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile


SWIM
TI


SESAR
JOINT UNDERTAKING

4.3.6 Safety requirements

This section provides safety requirements derived from analysis described in §4.2.2.1.

[REQ]

Identifier	REQ-17.01-TS-0300.0010
Title	Air SWIM Purple profile safe integration with avionics system
Requirement	Air SWIM Purple profile integration to avionics system shall remain compatible with existing aircraft type certificate(s).
Status	<validated>
Rationale	Taking into account that avionics systems installed on aircrafts' holding a Type Certificate (TC) have already been recognised compliant to EASA §1309 (either by ARP4754 Assurance level under POA, or by eTSO under A-DOA, approval), an initial safety objective is assumed to be: - Ensure that any operational (i.e. SWIM Enabled) service(s) intended to be operated over the SWIM Purple profile for advisory information sharing have been evaluated by a reference authority as having no safety effect on civil air transport operations. - Ensure that SWIM Purple profile integration with avionics system does not adversely impact existing aircraft type certificate(s). Targeting a minimal impact installation that is not increasing avionics systems complexity, so that any required Supplemental type certification (STC) only addresses none, or minor changes.
Category	<Safety>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0300.0015
Title	Air transport operations over SWIM Purple profile for advisory information sharing
Requirement	Operational/SWIM enabled service(s) intended to be operated over the SWIM Purple profile for advisory information sharing shall have been evaluated by a reference authority as having no safety effect on air transport certificate holders' operations.
Status	<in progress>
Rationale	Taking into account that avionics systems installed on aircrafts' holding a Type Certificate (TC) have already been recognised compliant to EASA §1309 (either by ARP4754 Assurance level under POA, or by eTSO under A-DOA, approval), an initial safety objective is assumed to be: - Ensure that any operational (i.e. SWIM Enabled) service(s) intended to be operated over the SWIM Purple profile for advisory information sharing have been evaluated by a reference authority as having no safety effect on civil air transport operations. - Ensure that SWIM Purple profile integration with avionics system does not adversely impact existing aircraft type certificate(s). In accordance with PJ.17 PMP, PJ.17-01 solution does not provide safety analysis, therefore only non-safety related services can be operated over SWIM PP assuming the aircraft airworthiness is not impaired (AIR.OPS.1). No safety effect: Failure conditions that would have no effect on safety (per AMC 25.1309).
Category	<Safety>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0300.0020
Title	Flight crew workload
Requirement	Any procedures associated with the control and monitoring of Air SWIM Purple profile Node for advisory information sharing should not result in unacceptable flight crew workload.
Status	<validated>
Rationale	Foreseen SWIM operational services, for which human performance and impact on crew resource monitoring have not been evaluated, do not allow evaluating flight crew workload and performance. As a result, the above requirement, in addressing EASA CS 2x.1302, aims at establishing an initial human factor objective.
Category	<Safety>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0300.0025
Title	Aircraft data domains segregation and message filtering policies
Requirement	Subject, context and content based SWIM message filtering policies definition and enforcement shall respect the data domain segregation per aircraft type design configuration.
Status	<validated>
Rationale	Aircraft domain reference model is specified in ARINC Report 664 P5 Aircraft Data Network which provides a notional model of the aircraft networking among four domains. Filtering and routing to avionics system must be done accordingly to the aircraft type design configuration, and with respect to data domain segregations.
Category	<Safety>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Filtering Purple Profile

4.3.7 Interface requirements

This section provides the interface requirements derived from the technical view described in §4.2.2 and in particular interface bindings as described in §4.2.2.5.

4.3.7.1 Purple Profile enabled SWIM Services bindings

[REQ]

Identifier	REQ-17.01-TS-1000.0010
Title	Air Purple Profile SWIM Node interface with avionics' systems
Requirement	Air Purple Profile SWIM Node shall interface with the avionics system in compliance with ARINC 834 ADIF.
Status	<validated>
Rationale	An aircraft network that is intended to be ARINC Report 821 or 828 compliant should provide an avionics interface service defined by ARINC Specification 834: Aircraft Data Interface Function (ADIF). The ADIF service defines programmatic communication protocols between network applications and aircraft avionics.
Category	<Interface>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-1000.0015
Title	Avionics' systems parameters accessed by the Air Purple Profile SWIM Node
Requirement	Air Purple Profile SWIM Node shall recover the following standard Aircraft parameters: - Airborne status, discrete word, 0: ground condition. - Time GMT, 0.01s resolution. - Position, 0.000172 nm resolution.
Status	<validated>
Rationale	Airborne status may be required to manage Air Purple Profile SWIM Node maintenance mode (upload of policies, certificates, …). Time is require to timestamp messages. Position may be required to optimize the selection of the most appropriate Ground SWIM Node, according to operator preferences. Applications designed for use on multiple aircraft types should verify that required generic parameters recovery is available on the current aircraft.
Category	<Interface>
Profile Part	<PP Air>
Domain of Interest	<SLA><Governance>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0100
Title	FDRR-MEP message exchange pattern federation
Requirement	The message distribution and routing federating the FDRR-MEP message exchange pattern shall comply with the design described in the messaging technical viewpoint.
Status	<validated>
Rationale	AMQP 1.0 is a wire level protocol for business messaging. The standard is suitable for all common business messaging behaviors and MEPs. The standard does not specify how to realize such MEPs but it provides a lower level peer-to-peer protocol on top of which is possible to build all common MEPs. In particular the standard does not mandate how to realize Publish/Subscribe MEPs or Request/Response MEPs. Permanent need for time, space and synchronization decoupling for all the Purple Profile technical use cases represents the main design constraint impacting the technical view of the messaging and in particular the message distribution function (related to MEPs). All the MEPs and technical use cases are realized over asynchronous messaging-based distributed intermediary aiming at decoupling aircraft and ground Purple Profile enabled applications in time, space and synchronization and dealing with additional constraints. This intermediary consists of interconnected and federated Air and Ground SWIM Nodes. The federated messaging entities are Message Queue, Message Topic and Subscription handler. Message distribution and routing aiming at federating the MEP, have to comply with Purple Profile technical view (§4.2.2.2.1).
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0010.0070

<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0055
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0065

[REQ]

Identifier	REQ-17.01-TS-0600.0105
Title	FDRMR-MEP message exchange pattern federation
Requirement	The message distribution and routing federating the FDRMR-MEP message exchange pattern shall comply with the design described in the messaging technical viewpoint.
Status	<validated>
Rationale	AMQP 1.0 is a wire level protocol for business messaging. The standard is suitable for all common business messaging behaviors and MEPs. The standard does not specify how to realize such MEPs but it provides a lower level peer-to-peer protocol on top of which is possible to build all common MEPs. In particular the standard does not mandate how to realize Publish/Subscribe MEPs or Request/Response MEPs. Permanent need for time, space and synchronization decoupling for all the Purple Profile technical use cases represents the main design constraint impacting the technical view of the messaging and in particular the message distribution function (related to MEPs). All the MEPs and technical use cases are realized over asynchronous messaging-based distributed intermediary aiming at decoupling aircraft and ground Purple Profile enabled applications in time, space and synchronization and dealing with additional constraints. This intermediary consists of interconnected and federated Air and Ground SWIM Nodes. The federated messaging entities are Message Queue, Message Topic and Subscription handler. Message distribution and routing aiming at federating the MEP, have to comply with Purple Profile technical view (§4.2.2.2.1).
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0010.0070
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0060
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0065

[REQ]

Identifier	REQ-17.01-TS-0600.0110
Title	PS*-MEP message exchange patterns federation
Requirement	The message distribution and routing federating the PS*-MEP message exchange patterns shall comply with the design described in the messaging technical viewpoint.
Status	<validated>
Rationale	AMQP 1.0 is a wire level protocol for business messaging. The standard is suitable for all common business messaging behaviors and MEPs. The standard does not specify how to realize such MEPs but it provides a lower level peer-to-peer protocol on top of which is possible to build all common MEPs. In particular the standard does not mandate how to realize Publish/Subscribe MEPs or Request/Response MEPs. Permanent need for time, space and synchronization decoupling for all the Purple Profile technical use cases represents the main design constraint impacting the technical view of the messaging and in particular the message distribution function (related to MEPs). All the MEPs and technical use cases are realized over asynchronous messaging-based distributed intermediary aiming at decoupling aircraft and ground Purple Profile enabled applications in time, space and synchronization and dealing with additional constraints. This intermediary consists of interconnected and federated Air and Ground SWIM Nodes. The federated messaging entities are Message Queue, Message Topic and Subscription handler. Message distribution and routing aiming at federating the MEP, have to comply with Purple Profile technical view (§4.2.2.2.1).
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0010.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0010.0050
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0005
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0010
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0015
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0020

[REQ]

Identifier	REQ-17.01-TS-0600.0115
Title	Subscription management operations
Requirement	The Subscription handler shall be able to handle messages concerning following subscription management operations: - subscription, - unsubscription, - active subscriptions retrieving.
Status	<validated>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). Basic subscription management requires the ability to handle (route, process) following pairs of subscription management messages: - SubscriptionRequest and SubscriptionResponse: subscription request operation

	allows applications to indicate the interest in receiving publication messages concerning a given SWIM service over Publish/Subscribe. - UnsubscriptionRequest and UnsubscriptionResponse: unsubscription request operation allows applications to terminate active subscriptions. - ActiveSubscriptionsRequest and ActiveSubscriptionsResponse: active subscriptions retrieving operation allows applications to retrieve their active subscriptions. This operation does not require specific message flow (federation logics) between aircraft and ground messaging; it is realized by relying on local (aircraft or ground) information concerning active subscriptions.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0025
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0030
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0035
<SPECIALIZES>	<ATMS Requirement>	REQ-17.01-TS-0010.0040

[REQ]

Identifier	REQ-17.01-TS-0600.0120
Title	Advanced Subscription management operations
Requirement	In addition to basic operations, the Subscription handler shall be able to handle

	messages concerning following advanced subscription management operations: - active subscription renewal, - subscription filter update.
Status	<validated>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). In addition to basic operations, advanced subscription management requires the ability to handle (route, process) following pairs of subscription management messages: - SubscriptionRenewRequest and SubscriptionRenewResponse: active subscription renewal allows applications to renew active subscriptions. - UpdateSubscriptionFilterRequest and UpdateSubscriptionFilterResponse: this request message allows applications to update the filtering criteria (if any) provided at subscription time. This is not applicable to Topic Expression and Producer Properties Selector: it is restricted only to Message Content Selector.
Category	<Interface>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0123
Title	Active Subscriptions Notify Subscription management operation
Requirement	In addition to basic operations, the Subscription handler shall be able to handle ActiveSubscriptionsNotify message.
Status	<in progress>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). In addition to basic operations, advanced subscription management requires the ability to handle (notify, process) the ActiveSubscriptionsNotify message. For downlink Publish/Subscribe services, It is up to the subscription handler on the Ground Purple Profile SWIM Node side to handle subscription management messages but it is also responsible to inform concerned subscription handlers on-board of the publishing aircraft about relevant subscription management events. The subscription handlers on-board of the publishing aircraft are not responsible for accepting/rejecting the subscription management messages but they have to make sure that messages are published according to active subscriptions (e.g. no needs to downlink messages if there are no active subscriptions). The ActiveSubscriptionsNotify message (one-way, no responses are required) is the message used by the subscription handler on the Ground Purple Profile SWIM Node side to notify concerned Air side subscription handlers. This message can be sent periodically or triggered by subscription updates (e.g. unsubscription, subscription renew, etc.).
Category	<Interface>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0125
Title	Subscription management operations messages XSD
Requirement	Subscription, unsubscription and active subscriptions retrieving request and response AMQP application-data section XML content shall comply with respective message structure defined in the subscription management XSD.
Status	<validated>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). In order to promote semantic and technical interoperability, the XML schema (XSD) for subscription management messages has been defined. This requirement concerns messages related to basic subscription management operations. Subscription management request and response AMQP message application-data section is an amqp-value holding a string representation of the XML.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0130
Title	Advanced Subscription management operations messages XSD
Requirement	Active subscription renewal and subscription filter update request and response AMQP application-data section XML content shall comply with respective message structure defined in the subscription management XSD.
Status	<validated>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). In order to promote semantic and technical interoperability, the XML schema (XSD) for subscription management messages has been defined. This requirement concerns messages related to advanced subscription management operations. Subscription management request and response AMQP message application-data section is an amqp-value holding a string representation of the XML.
Category	<Interface>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0135
Title	Subscription management operations messages end to end integrity and authenticity
Requirement	End to end message integrity and authenticity of subscription management messages shall be secured via digital signature detached from the application-data section.
Status	<validated>
Rationale	The Purple Profile defines the federated Publish/Subscribe MEP. The subscription management is based on asynchronous messaging and in particular on FDRR-MEP: subscription messages distribution is realized as for Request/Response services (the responder is the subscription handler responsible for accepting or not the subscription management request messages). Most of the subscription management request messages are routed to the intended subscription handler via distribution nodes (subscription management request and response AMQP message application-data section is an amqp-value holding a string representation of the XML). This is why message level integrity and authenticity have to be secured. Currently the design decision is to use the detached form for message level security provided by the Purple Profile (AMQP footer section). Request messages are signed using requestor's private key and verified by the responder using requestor's public key. Response messages are signed using responder's private key and verified by the requestor using responder's public key.
Category	<Interface><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0290.0020

[REQ]

Identifier	REQ-17.01-TS-0600.0245
Title	Fallback option for message level information security transfer for security information detached from the data
Requirement	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to transfer information security using the AMQP footer, the following fallback solution should be provided: - Use the AMQP application properties section instead of the AMQP footer section, or both. - AMQP application properties containing same <key,value> pairs defined for AMQP footer. - Usage and further details concerning the fallback solution are documented. - When possible, to avoid to transfer over the Air/Ground connection the security information duplicated in AMQP application properties and footer sections.
Status	<in progress>
Rationale	The Purple Profile provides two mechanisms to transfer message level security information from the sender to the intended recipient(s): - Security information attached to the data: the application-data section within the AMQP bare message includes both data and security information (e.g. digital signature). Examples of applicable standards are S/MIME 3.2, XML signature and XML encryption. - Security information detached from the data: the application-data section within the AMQP bare message includes plain or encrypted data and cryptographic information (message digest, digital signature, etc.) are included in the AMQP 1.0 footer section. This requirement concerns the message level security information transfer for security information detached from the data form. During technical validation activities some EXEs reported third-party software limitations in properly handling/transferring the AMQP footer. In order to maximize technical interoperability (point to point and end to end), a fallback option based on the use of AMQP application properties section is allowed. It is based on the use of application properties with same <key,value> pairs defined for AMQP footer. For instance, for the digital signature, the application key/name is DSGN and the value is the semicolon separated DSGN-Algorithm, DSGN-Target and DSGN-Signature. This option mainly impacts amqp peers: both sender and receiver have to implement (when needed) this fallback option. The use and needs of this option could be dynamically discovered at run-time (e.g. the receiving peer tries to retrieve the information first from the AMQP footer and then from the application properties) and/or documented off-line (configuration phase). In order to optimize the use of Air/Ground network/data links, it is recommended to

Company General Use

	try to avoid to transfer over the Air/Ground connection the security information duplicated in AMQP application properties and footer sections. This should be handled at configuration time and per Air SWIM Node – Ground SWIM Node pair (e.g. when connected to multiple Ground SWIM Node, for each "connection" the Air SWIM Node may transfer the security information using the footer or the application properties section.
Category	<Interface><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0280.0015
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0290.0015
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0290.0020
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0135

[REQ]

Identifier	REQ-17.01-TS-0600.0005
Title	AMQP 1.0 based instantiation of messaging entities
Requirement	Instantiation over AMQP 1.0 of the messaging entities shall comply with the design described in the messaging technical viewpoint.

Status	<validated>
Rationale	AMQP 1.0 is a wire level protocol for business messaging. The standard is suitable for all common business messaging behaviors and MEPs. The standard does not specify how to realize such MEPs but it provides a lower level peer-to-peer protocol on top of which is possible to build all common MEPs. In particular the standard does not mandate how to realize Publish/Subscribe MEPs or Request/Response MEPs. These considerations are applicable also to the applicable messaging entities defined in the messaging characterization. The Purple Profile aims at providing a technical layer enabling technical interoperability: building on top of the openness of AMQP 1.0 a concrete instantiation of Publish/Subscribe MEPs and Request/Response MEPs is designed and specified. The reference instantiation over AMQP 1.0 of the applicable messaging entities is described in the Purple Profile messaging technical viewpoint (§4.2.2.2.2).
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable><Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0140
Title	On-the-fly compression QoS over AMQP 1.0
Requirement	SWIM-TI level on-the-fly compression QoS over AMQP 1.0 shall be instantiated as

	follows: + AMQP data section size threshold based compression. + AMQP peer compressing the data has to add the on-the-fly-compressed AMQP message annotation. + AMQP peer uncompressing the data has to rely on the on-the-fly-compressed AMQP message annotation value. + The on-the-fly-compressed AMQP message annotation has to be in accordance with following key-value pair: - key: x-ontheflycompressed - value: {gzip|deflate}.
Status	<validated>
Rationale	Data compression can be realized in more than one way and at distinct levels. The ATM application layer can provide a compressed payload to the SWIM-TI. In this case (perimeter between ATM and SWIM-TI layers) the TI is only responsible for routing the message to the intended recipients. However, content-type and content-encoding properties have to be used in accordance with the AMQP 1.0 standard §3.2.4. The SWIM-TI itself can also provide data compression (on-the-fly compression). This is an advanced capability that could be useful when application level messages are not optimized in terms (e.g.) of message size for the uplink . Examples could be uplink of AIXM or WXXM data from the ground in a many to many information exchange: irrespective of A/C specific filtering criteria such data could be published and available for aircraft and ground applications: the publisher is not implementing subscribers specific data representation. In this case, the messages between Air and Ground SWIM Node could be compressed on-the-fly in a way transparent to the publisher and subscriber: the publisher publishes uncompressed message and the aircraft subscriber receives an uncompressed message. The TI is handling the payload as a sequence of bytes compressing and uncompressing it when needed (threshold based compression is supported). The message-annotations section is required when the on-the-fly QoS is configured at SWIM-TI level. One annotation is defined: it indicates that the payload (Bare Message Application Data) has been compressed on the fly by a distribution node. In accordance with AMQP 1.0 core, on receiving this annotation key, if not supported the receiving AMQP container MUST detach the link with a not-implemented error. However this should never occur because all the messaging resources and capabilities are agreed and configured in advance. The value indicates the compression algorithm used. The receiving AMQP peer relies on this annotation to evaluate if the message has been compressed (the AMQP message contains the annotation) and which algorithm has been used.
Category	<Interface>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>

Company General Use

Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0145
Title	AMQP 1.0 annotated message header section
Requirement	AMQP 1.0 annotated message shall contain one AMQP 1.0 header section used as follows: + durable field: set to true when durable message durability QoS is used. + priority field: integer (min inclusive value = 0, max inclusive value = 9, default priority = 4). + ttl field: mandatory. It is the lifespan relative to the message creation time property. + first-acquirer field: not used. + delivery-count field: may be used to discover maximum number of retries.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the header section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 header section. Furthermore, this requirement provides also additional constraints and clarifications concerning the header section fields.
Category	<Interface>
Profile Part	<PP Core>

Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0150
Title	AMQP 1.0 annotated message properties section
Requirement	AMQP 1.0 annotated message shall contain one AMQP 1.0 properties section used as follows: + all the fields are mandatory and used except group-id, group-sequence and reply-to-group-id.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section fields.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0155
Title	AMQP 1.0 annotated message properties section: message-id
Requirement	The AMQP 1.0 properties section message-id field shall be set as follows: + String representation of UUID variant 2 version 4 (random) as defined in the IETF RFC 4122. + AMQP-UUID type as defined in AMQP 1.0 core §3.2.12.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the message-id field. It has to be noted that all the restrictions described in the AMQP 1.0 core §3.2.4 are applicable (uniqueness, under message producer responsibility, properties must remain unaltered when retransmitted).
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0160
Title	AMQP 1.0 annotated message properties section: user-id
Requirement	The AMQP 1.0 properties section user-id field shall be set as follows: + message producer's Name-Based UUID as defined in the IETF RFC 4122 and derived/generated as follows: - Name: the X.500 Distinguished Names (DNs) from the entity's X.509v3 certificate. - Namespace: X.500 DN with namespace UUID "6ba7b814-9dad-11d1-80b4-00c04fd430c8" (IETF RFC 4122).
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the user-id field. It has to be noted that all the restrictions described in the AMQP 1.0 core §3.2.4 are applicable.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0010.0080
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0010.0085

[REQ]

Identifier	REQ-17.01-TS-0600.0250
Title	Fallback option for AMQP annotated message user-id property
Requirement	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the user-id property, the following fallback solution should be provided: + Add the user-id information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “userid”. - value = string representation of the name-based UUID. + Usage and further details concerning the fallback solution are documented.
Status	<in progress>
Rationale	During technical validation activities some EXEs reported third-party software limitations in properly handling/transferring/retaining point to point or/and end to end the original AMQP user-id property. In order to maximize technical interoperability (point to point and end to end), a fallback option based on the use of AMQP application properties section is allowed.
Category	<Interface>

Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0160

[REQ]

Identifier	REQ-17.01-TS-0600.0165
Title	AMQP 1.0 annotated message properties section: to
Requirement	The AMQP 1.0 properties section "to" field shall be used as follows: + required but AMQP 1.0 core addressing scheme(s) not constrained nor standardized. + Addressing scheme has to be documented as part of the binding's contract. + Purple Profile implementations may use addresses syntax and semantics described in the latest working draft for OASIS AMQP Addressing. + The Purple Profile messaging may use this field for routing purposes.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties

	section and in particular on the to field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0170
Title	AMQP 1.0 annotated message properties section: subject
Requirement	The AMQP 1.0 properties section subject field shall be used as follows: + required but the template (syntax, semantics) is not constrained nor standardized except for subscription management messages. + the Purple Profile messaging may use this section for filtering and routing purposes. + The syntax and semantics have to be documented as part of the binding's contract.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the subject field.

Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0175
Title	AMQP 1.0 annotated message properties section: subject for subscription management messages
Requirement	The AMQP 1.0 properties section subject field for subscription management messages shall be set as follows: + SubscriptionRequest: - https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRequest + SubscriptionResponse: - https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionResponse + UnsubscriptionRequest: - https://sesarju.eu/swim/PP/SubscriptionManagement:UnsubscriptionRequest + UnsubscriptionResponse: - https://sesarju.eu/swim/PP/SubscriptionManagement:UnsubscriptionResponse

	+ SubscriptionRenewRequest: - https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRenewRequest + SubscriptionRenewResponse: - https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRenewResponse + UpdateSubscriptionFilterRequest: - https://sesarju.eu/swim/PP/SubscriptionManagement:UpdateSubscriptionFilterRequest + UpdateSubscriptionFilterResponse: - https://sesarju.eu/swim/PP/SubscriptionManagement:UpdateSubscriptionFilterResponse + ActiveSubscriptionsRequest: - https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsRequest + ActiveSubscriptionsResponse: - https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsResponse +ActiveSubscriptionsNotify: - https://sesarju.eu/swim/PP/SubscriptionManagement:ActiveSubscriptionsNotify
Status	<validated>
Rationale	The Purple profile standardizes the subjects to be used for subscription management request and response messages (e.g. for SubscriptionRequest message the subject must be https://sesarju.eu/swim/PP/SubscriptionManagement:SubscriptionRequest).
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0180
Title	AMQP 1.0 annotated message properties section: reply-to
Requirement	The AMQP 1.0 properties section "reply-to" field shall be used as follows: + required for request messages only including subscription management. + AMQP 1.0 core addressing scheme(s) not constrained nor standardized + Addressing scheme has to be documented as part of the binding's contract. + Purple Profile implementations may use addresses syntax and semantics described in the latest working draft for OASIS AMQP Addressing. + The Purple Profile messaging may use this field for routing purposes.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the reply-to field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0185
Title	AMQP 1.0 annotated message properties section: correlation-id
Requirement	The AMQP 1.0 properties section correlation-id field shall be used as follows: + required for response messages only including subscription management. + set to message-id of correlated (request) message.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the correlation-id field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0190
Title	AMQP 1.0 annotated message properties section: content-type
Requirement	The AMQP 1.0 properties section content-type field shall be used as follows: + required. + set to the applicable IETF RFC 2046 MIME Media type. + to be documented as part of the binding's contract.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the content-type field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0255
Title	Fallback option for AMQP annotated message content-type property
Requirement	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the content-type property, the following fallback solution should be provided: + Add the content-type information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “contentType”. - value = string representation of the applicable IETF RFC 2046 MIME Media. + Usage and further details concerning the fallback solution are documented.
Status	<in progress>
Rationale	During technical validation activities some EXEs reported third-party software limitations in properly handling/transferring/retaining point to point or/and end to end the original AMQP content-type property. In order to maximize technical interoperability (point to point and end to end), a fallback option based on the use of AMQP application properties section is allowed.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0190
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0200

[REQ]

Identifier	REQ-17.01-TS-0600.0195
Title	AMQP 1.0 annotated message properties section: content-encoding
Requirement	The AMQP 1.0 properties section content-encoding field shall be used as follows: + as per section 3.5 of RFC 2616 and used to provide compression standards info used to compress original application-data sections. + set to - “gzip”: GZIP (RFC 1952) compressed original MIME type. - “deflate”: Deflate (RFC 1951) compressed original MIME type inside the zlib data format (RFC 1950). + used in conjunction with content-type as per AMQP 1.0 - when present (compressed data), the content-type must be "application/octet-stream".
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the content-encoding field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0260
Title	Fallback option for AMQP annotated message content-encoding property
Requirement	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the content-encoding property, the following fallback solution should be provided: + Add the content-encoding information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “contentEncoding”. - value = in accordance with REQ-17.01-TS-0600.0195. + Usage and further details concerning the fallback solution are documented.
Status	<in progress>
Rationale	During technical validation activities some EXEs reported third-party software limitations in properly handling/transferring/retaining point to point or/and end to end the original AMQP content-encoding property. In order to maximize technical interoperability (point to point and end to end), a fallback option based on the use of AMQP application properties section is allowed.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0195
<APPLIES_TO>	<ATMS Requirement>	REQ-17.01-TS-0600.0200

[REQ]

Identifier	REQ-17.01-TS-0600.0200
Title	AMQP 1.0 annotated message properties section: content-type for subscription management messages
Requirement	The AMQP 1.0 properties section content-type field for subscription management messages shall be set to "application/xml".
Status	<validated>
Rationale	The Purple profile standardizes the content-type to be used for subscription management request and response messages. Taking into account the required content-type, the Purple profile subscription management request and response messages are not compressed (i.e. content-encoding field is not used for subscription management messages).
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Subscription handler><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0205
Title	AMQP 1.0 annotated message properties section: absolute-expiry-time
Requirement	The AMQP 1.0 properties section absolute-expiry-time field shall be used as follows: + required. + the absolute point in time when the message is considered expired. + restricted to milliseconds since the Unix Epoch.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the absolute-expiry-time field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0210
Title	AMQP 1.0 annotated message properties section: creation-time
Requirement	The AMQP 1.0 properties section creation-time field shall be used as follows: + required. + the absolute point in time when the message was created. + restricted to milliseconds since the Unix Epoch.
Status	<validated>
Rationale	In accordance with AMQP 1.0, it is not mandatory that an annotated message contains the properties section. Purple Profile is relying on this section and all the AMQP messages (publication messages, request messages, subscription request, etc.) have to contain the AMQP 1.0 properties section. Furthermore, this requirement provides also additional constraints and clarifications concerning the properties section and in particular on the creation-time field.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0215
Title	AMQP 1.0 annotated message application-data section
Requirement	AMQP 1.0 annotated message shall contain one application-data section (body) consisting either of one data section or a single amqp-value section.
Status	<validated>
Rationale	In accordance with AMQP 1.0, for the application-data section (body) three choices exist: one or more data sections, one or more amqp-sequence sections, or a single amqp-value section. The Purple Profile introduces constraints allowing only data section and amqp-value options (i.e. amqp-sequence sections are not allowed). Although it is not strictly in scope of this specification, some guidance/suggestions have been identified when using third-party software based on JMS – AMQP mapping. On top of the constraints on the AMQP application-data section (only one data section or a single amqp-value) specified in this requirement, the Purple Profile only does constrain the application-data section for subscription management request and response messages. In particular, the subscription management request and response AMQP message application-data section is an amqp-value holding a string representation of the XML. In all the other cases, details about application-data section use are part of the SWIM service contract description (contract section of the interface bindings). When using third-party software based on JMS – AMQP mapping it is recommended to review both third-party software documentation and OASIS (working draft, April 2017) Advanced Message Queuing Protocol (AMQP) JMS Mapping §3.2.4. Any further limitations or/and constraints impacting technical interoperability, have to be properly documented as part of the SWIM service interface binding contract.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0220
Title	AMQP 1.0 annotated message application-properties section
Requirement	When present, the AMQP 1.0 annotated message application-properties section shall be used as follows: - not standardized by the Purple Profile. - properties to be documented as part of the binding's contract. - Purple Profile messaging may use this section for filtering and routing purposes. - AMQP 1.0 core filter restricted to http://www.amqp.org/specification/1.0/filters, APACHE.ORG:SELECTOR capability.
Status	<validated>
Rationale	AMQP 1.0 annotated message application-properties section (when present) may be used to enforce subject based filtering (e.g. Message Content selector) and routing in accordance with applicable messaging policies.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Responder><Requestor>
Selfstanding set	<Not applicable>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0010
Title	TCP RFC 793 Interoperability standard
Requirement	The SWIM Node shall support IETF RFC 793 Transmission Control Protocol September 1981 http://tools.ietf.org/html/rfc793.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. AMQP 1.0 and CA/PKI bindings rely on TCP/IP connections.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0070
Title	XML 1.0 Fifth Edition interoperability standard
Requirement	The SWIM Node shall support W3C Recommendation Extensible Markup Language (XML) 1.0 (Fifth Edition) 26 November 2008 http://www.w3.org/TR/xml/.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. XML is used for subscription management messages.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0075
Title	XML 1.0 Fourth Edition interoperability standard
Requirement	The SWIM Node shall support W3C Recommendation Extensible Markup Language (XML) 1.0 (Fourth Edition) 16 August 2006, edited in place 29 September 2006 http://www.w3.org/TR/2006/REC-xml-20060816/.
Status	<validated>

Rationale	Compliance with well-known and widely used standard promotes interoperability. XML is used for subscription management messages.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0080
Title	XML Schema 1.0 interoperability standard
Requirement	The SWIM Node shall support W3C Recommendation XML Schema Part 1: Structures Second Edition 28 October 2004 http://www.w3.org/TR/xmlschema-1/ and W3C Recommendation XML Schema Part 2: Datatypes Second Edition 28 October 2004 http://www.w3.org/TR/xmlschema-2/.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. XML is used for subscription management messages.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0135
Title	AMQP 1.0 interoperability standard
Requirement	The SWIM Node shall support ISO/IEC 19464: 2014 Information technology Advanced Message Queuing Protocol (AMQP) v1.0 specification, First Edition 2014-05-01http://standards.iso.org/ittf/PubliclyAvailableStandards/c064955_ISO_IEC_19464_2014.zip.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This ISO/IEC standard is the OASIS standard Advanced Message Queuing Protocol (AMQP) Version 1, 29 October 2012. Purple Profile messaging is based on higher level messaging functionality over AMQP 1.0. The support of this standard is constrained and limited according to the "constraints" sections defined in the AMQP 1.0 based Purple Profile interface bindings.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0160
Title	MIME Media Type interoperability standard
Requirement	The SWIM Node shall support IETF RFC 2046 Multipurpose Internet Mail Extensions (MIME) Media Types https://www.ietf.org/rfc/rfc2046.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. MIME Media Type is used for AMQP 1.0 messages content type and encoding.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0180
Title	UUID interoperability standard
Requirement	The SWIM Node shall support IETF RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace https://www.ietf.org/rfc/rfc4122.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. UUIDs are used for AMQP 1.0 message-id (UUID) and user-id (name-Based UUID) properties.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0185

Title	URI interoperability standard
Requirement	The SWIM Node shall support IETF RFC 3986 Uniform Resource Identifier (URI), Generic Syntax https://www.ietf.org/rfc/rfc3986.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. URIs are used AMQP 1.0 to and reply-to properties.
Category	<Interface><Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0165
Title	GZIP interoperability standard
Requirement	The SWIM Node shall support IETF RFC 1952 GZIP file format specification version 4.3 https://www.ietf.org/rfc/rfc1952.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. GZIP is used for on-the-fly compression QoS: both Air and Ground SWIM Nodes have to be able to deal with this standard (typically compression happens on the ground and decompression happens on the air at SWIM-TI layer).

Category	<Interface><Interoperability>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0170
Title	DEFLATE Compression interoperability standard
Requirement	The SWIM Node shall support IETF RFC 1951 DEFLATE Compressed Data Format Specification version 1.3 https://www.ietf.org/rfc/rfc1951.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. DEFLATE is used for on-the-fly compression QoS: both Air and Ground SWIM Nodes have to be able to deal with this standard (typically compression happens on the ground and decompression happens on the air at SWIM-TI layer).
Category	<Interface><Interoperability>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0175
Title	ZLIB Compression interoperability standard
Requirement	The SWIM Node shall support IETF RFC 1950 ZLIB Compressed Data Format Specification version 3.3 https://www.ietf.org/rfc/rfc1950.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. DEFLATE (zlib data format) is used for on-the-fly compression QoS: both Air and Ground SWIM Nodes have to be able to deal with this standard (typically compression happens on the ground and decompression happens on the air at SWIM-TI layer).
Category	<Interface><Interoperability>
Profile Part	<PP Air Advanced><PP Ground Advanced>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0600.0225
Title	Publish/Subscribe over AMQP binding
Requirement	Subscription management and message distribution functions shall be provided over the Publish/Subscribe over AMQP binding characterized as follows: + Protocol stack: - Stacking: Publish/Subscribe Messaging Entities Purple Profile messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides publication message distribution and subscription management for the federated PSPUSH-MEP and PSPULL-MEP. - Operations: AMQP 1.0 connection, session and link are initiated by the AMQP peer using an instance of this binding. Sending publication message/subscription management request message: . Sender entity establishes an AMQP 1.0 link with the MT/Subscription handler's request MQ made available by this binding with "source" link type (link type on the MT/Subscription handler's request MQ side is "target"). Receiving publication message/subscription management response message: . Receiver entity establishes an AMQP 1.0 link with the MT/Subscription management response MQ made available by this binding with "target" link type (link type on the MT/ Subscription management response MQ side is "source"). - Message structure& format: the AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: . one header section. . one properties section. . one application-data section (body) consists of one data section or a single amqp-value section. . zero or one footer section.

	- Fault/failure/error: in accordance with AMQP 1.0 core. - Constraints: . Additional messaging functionalities are required on top of AMQP 1.0 core to fulfil Purple Profile design. . TLS 1.3 (amqps form only) is required but fallback to 1.2 is allowed. . The binding can be instantiated over IPv4 or IPv6. . AMQP 1.0 core transactions are not used. . Fixed range for the idle-time-out parameter of the AMQP open performative . The binding constrains the sections of the AMQP 1.0 annotated message. . The binding is instantiated and configured according to the elements described in the contract section. . AMQP 1.0 core filter restricted to http://www.amqp.org/specification/1.0/filters, APACHE.ORG:SELECTOR capability. + Security: - Authentication: . Point to point: mutual transport level authentication of AMQP 1.0 peers through TLS {1.2|1.3} according to the amqps form only. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Authorization: . Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the binding. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Integrity: . Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Confidentiality: . Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s).

Company General Use

	- Non-repudiation: . Point to point: audit logging. . End to end: depending on the message level security controls used by the specific service. + QoS: - Delivery guarantees: the binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile. - Lifetime: message with specified lifespan, Non-Temporary Topic, Non-Temporary Queue (Subscription management), subscription with unspecified lifetime and (optionally) subscription with specified lifetime. - Durability: when not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message topics, {durable | non-durable } subscription and { volatile | durable} subscription handler are supported. - Ordering guarantees: {FIFO | Best effort message priority} message ordering guarantees are provided. - CoSs: the instantiation of this binding allows to assign a specific class of service. + Contract: - Addressing: the binding does not constrain nor standardize the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for message topics and subscription management request and response message queues. - Messaging resources: message topics and subscription management message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of these resources. - Messaging Policies: messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation. - Security Policies: security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured. - QoSs: the instantiation of this binding requires that the applicable QoSs are documented and configured. - CoS: the instantiation of this binding requires that the applicable CoS is documented

	and configured. - Application-data: Although it is opaque for the binding, in order to enabled end to end interoperability the physical information model (e.g. JSON schema, XSDs, etc.) for publication message has to be documented. Purple Profile provides XML schema for subscription management request and response messages. - Application properties: The binding can use these properties for filtering and routing purposes. However, even if not used by the binding, in order to enabled end to end interoperability any application properties have to be documented. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding>. Aircraft side binding instances are stacked with <Network binding> over the Aircraft Information Network. Ground side are stacked with <Network binding> over the G/G Communication Network. - Relies on Publish/Subscribe over AMQP federation <Internal service binding>: the binding relies on Publish/Subscribe over AMQP federation bindings for MEP federation. - (optionally) Relies on CDP and/or OCSP bindings: The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.
Status	<validated>
Rationale	In accordance with Purple Profile technical viewpoint, Purple Profile enabled SWIM services are made accessible to the application layer (Purple Profile enabled SWIM applications) via a pair of bindings of type <Service binding> federated via a binding of type <Internal service binding>. In particular, the bindings triad for Purple Profile enabled SWIM service over PS*-MEP can be summarized as follows: - Message topics and subscription handler are made available via two "Publish/Subscribe over AMQP" <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network) and another on the ground side (stacked with <Network binding> over the G/G Communication Network). These bindings have to be instantiated according to the specific service (refer to the "contract" field) and directly accessed by SWIM enabled applications depending on the role (publisher, subscriber). Publication Registration Management function, when needed, it is realized via off-line exchange (e.g. SLA agreement and configuration) and not over <Service binding>. - Airborne and Ground <Service binding> message topics and subscription handlers are federated via "Publish/Subscribe over AMQP federation" <Internal service binding> (stacked with <Network binding> over the A/G Communication Network) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding is instantiated according to routing and segregation needs documented for each service (refer to TS §4.2.2.2.1). This requirement concerns the bindings of <Service binding> type for PS*-MEP and it has been defined in accordance with Purple Profile technical viewpoint (TS §4.2.2) and

Company General Use

	interface bindings template documented in the Purple Profile TS. In particular protocol stack, security, QoS, contract and binding relationships binding sections are described. In the Purple Profile TS §4.2.2.5 the same binding is described in a table form. The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding. Furthermore, it is anticipated that not all the applicable requirements are traced/included (e.g. QoS over AMQP requirements, reliability, message screening, AMQP over TLS requirements, etc.): conformance to this binding is not strictly covered only by the traced requirements.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Service binding>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0110
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0115
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0120

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0123
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0125
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0130
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0150
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0175
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0190
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0195
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0200
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0205
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0210
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0215
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0220
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0070
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0075
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0080
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0015

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0025
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055

[REQ]

Identifier	REQ-17.01-TS-0600.0230
Title	Publish/Subscribe over AMQP federation binding
Requirement	Subscription management and message distribution federation shall be provided over the Publish/Subscribe over AMQP federation binding characterized as follows: + Protocol stack: - Stacking: Publish/Subscribe Messaging Entities Purple Profile messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides publication message distribution and subscription management for the federated PSPUSH-MEP and PSPULL-MEP. - Operations: AMQP 1.0 connection, session and link are initiated by the AMQP peer (i.e. Air SWIM Node) using an instance of this binding. Sending publication message/subscription management request message: . Sender entity establishes an AMQP 1.0 link with the MT/Subscription handler's request MQ made available by this binding with "source" link type (link type on the MT/Subscription handler's request MQ side is "target"). Receiving publication message/subscription management response message: . Receiver entity establishes an AMQP 1.0 link with the MT/Subscription management response MQ made available by this binding with "target" link type (link type on the MT/ Subscription management response MQ side is "source"). - Message structure& format: the AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: . header, properties, application-data and footer from federated Publish/Subscribe over AMQP binding instance. . one message-annotations section in case on-the-fly compression is enabled/provided. - Fault/failure/error: in accordance with AMQP 1.0 core. - Constraints: same as for Publish/Subscribe over AMQP binding.

Company General Use

	+ Security: - Authentication: . Point to point: mutual transport level authentication of AMQP 1.0 peers (Air and ground SWIM Nodes) through TLS {1.2|1.3} according to the amqps form only. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Authorization: . Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the binding. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Integrity: . Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Confidentiality: . Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Non-repudiation: . Point to point: audit logging. . End to end: depending on the message level security controls used by the specific service. + QoS: - Delivery guarantees: the binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer (i.e. Air SWIM Node) ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile. - Lifetime: message with specified lifespan, Non-Temporary Topic, Non-Temporary Queue (Subscription management), subscription with unspecified lifetime and (optionally) subscription with specified lifetime. - Durability: when not constrained by the chosen delivery guarantee, {durable | non-

	durable} messages, and {non-durable | volatile | durable} message topics, {durable | non-durable } subscription and { volatile | durable} subscription handler are supported. - Ordering guarantees: {FIFO | Best effort message priority} message ordering guarantees are provided. - CoSs: the instantiation of this binding allows to assign a specific class of service. + Contract: - Addressing: the binding does not constrain nor standardize the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for message topics and subscription management request and response message queues. - Messaging resources: message topics and subscription management message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of these resources. - Messaging Policies: messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation. - Security Policies: security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured. - QoSs: the instantiation of this binding requires that the applicable QoSs are documented and configured taking into account QoSs of federated Publish/Subscribe over AMQP binding instances. - CoS: the instantiation of this binding requires that the applicable CoS is documented and configured taking into account CoS of the federated Publish/Subscribe over AMQP binding instances. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding> over the A/G Communication Network. - Federates Publish/Subscribe over AMQP binding <Service binding>: the binding provides messaging functionalities aiming at federating Publish/Subscribe over AMQP binding <Service binding> bindings pair(s). - (optionally) Relies on CDP and/or OCSP bindings: the binding optionally relies on (use with “consumer” role) CDP or/and OCSP for X.509v3 for certificate revocation status check.
Status	<validated>
Rationale	In accordance with Purple Profile technical viewpoint, Purple Profile enabled SWIM services are made accessible to the application layer (Purple Profile enabled SWIM applications) via a pair of bindings of type <Service binding> federated via a binding of

	type <Internal service binding>. In particular, the bindings triad for Purple Profile enabled SWIM service over PS*-MEP can be summarized as follows: - Message topics and subscription handler are made available via two "Publish/Subscribe over AMQP" <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network) and another on the ground side (stacked with <Network binding> over the G/G Communication Network). These bindings have to be instantiated according to the specific service (refer to the "contract" field) and directly accessed by SWIM enabled applications depending on the role (publisher, subscriber). Publication Registration Management function, when needed, it is realized via off-line exchange (e.g. SLA agreement and configuration) and not over <Service binding>. - Airborne and Ground <Service binding> message topics and subscription handlers are federated via "Publish/Subscribe over AMQP federation" <Internal service binding> (stacked with <Network binding> over the A/G Communication Network) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding is instantiated according to routing and segregation needs documented for each service (refer to TS §4.2.2.2.1). This requirement concerns the bindings of <Internal service binding> type for PS*-MEP and it has been defined in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. In particular protocol stack, security, QoS, contract and binding relationships binding sections are described. In the Purple Profile TS §4.2.2.5 the same binding is described in a table form. The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding. Furthermore, it is anticipated that not all the applicable requirements are traced/included (e.g. QoS over AMQP requirements, reliability, message screening, AMQP over TLS requirements, etc.): conformance to this binding is not strictly covered only by the traced requirements.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Internal service binding>

Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0110
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0140
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0150
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0175
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0190
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0195
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0200
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0205
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0210
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0215
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0220
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0070

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0075
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0080
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0175
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0025
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055

[REQ]

Identifier	REQ-17.01-TS-0600.0235
Title	Fully decoupled Request/Response over AMQP binding
Requirement	Request and Response message distribution function shall be provided over the Fully decoupled Request/Response over AMQP binding characterized as follows: + Protocol stack: - Stacking: Request/Response Messaging Entities Purple Profile messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides request and response messages distribution for the federated FDRR-MEP and FDRMR-MEP. - Operations: AMQP 1.0 connection, session and link are initiated by the AMQP peer using an instance of this binding. Sending request or response message: . Sender entity establishes an AMQP 1.0 link with the request (response) MQ made

	available by this binding with “source” link type (link type on the MQ side is “target”). Receiving request or response message: . Receiver entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with “target” link type (link type on the MQ side is “source”). - Message structure& format: the AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: . one header section. . one properties section. . one application-data section (body) consists of one data section or a single amqp-value section. . zero or one footer section. - Fault/failure/error: in accordance with AMQP 1.0 core. - Constraints: . Additional messaging functionalities are required on top of AMQP 1.0 core to fulfil Purple Profile design. . TLS 1.3 (amqps form only) is required but fallback to 1.2 is allowed. . The binding can be instantiated over IPv4 or IPv6. . AMQP 1.0 core transactions are not used. . Fixed range for the idle-time-out parameter of the AMQP open performative . The binding constrains the sections of the AMQP 1.0 annotated message. . The binding is instantiated and configured according to the elements described in the contract section. . AMQP 1.0 core filter restricted to http://www.amqp.org/specification/1.0/filters, APACHE.ORG:SELECTOR capability. + Security: - Authentication: . Point to point: mutual transport level authentication of AMQP 1.0 peers through TLS {1.2|1.3} according to the amqps form only. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Authorization: . Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available

	through the binding. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Integrity: . Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Confidentiality: . Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Non-repudiation: . Point to point: audit logging. . End to end: depending on the message level security controls used by the specific service. + QoS: - Delivery guarantees: the binding provides At-Most-Once. Optionally, it provides {At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile. - Lifetime: message with specified lifespan and Non-Temporary Queue. - Durability: when not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message queues are supported. - Ordering guarantees: {FIFO | Best effort message priority} message ordering guarantees are provided. - CoSs: the instantiation of this binding allows to assign a specific class of service. + Contract: - Addressing: the binding does not constrain nor standardize the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for request and response message queues. - Messaging resources: message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of

	message queues. - Messaging Policies: messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation. - Security Policies: security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured. - QoSs: the instantiation of this binding requires that the applicable QoSs are documented and configured. - CoS: the instantiation of this binding requires that the applicable CoS is documented and configured. - Application-data: although it is opaque for the binding, in order to enabled end to end interoperability the physical information model (e.g. JSON schema, XSDs, etc.) has to be documented. - Application properties: the binding can use these properties for filtering and routing purposes. However, even if not used by the binding, in order to enabled end to end interoperability any application properties have to be documented. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding>. Aircraft side binding instances are stacked with <Network binding> over the Aircraft Information Network. Ground side are stacked with <Network binding> over the G/G Communication Network. - Relies on Request/Response over AMQP federation <Internal service binding>: The binding relies on Request/Response over AMQP federation bindings for MEP federation. - (optionally) Relies on CDP and/or OCSP bindings: The binding optionally relies on (use with "consumer" role) CDP or/and OCSP for X.509v3 for certificate revocation status check.
Status	<validated>
Rationale	In accordance with Purple Profile technical viewpoint, Purple Profile enabled SWIM services are made accessible to the application layer (Purple Profile enabled SWIM applications) via a pair of bindings of type <Service binding> federated via a binding of type <Internal service binding>. In particular, the bindings triad for Purple Profile enabled SWIM service over FDRR-MEP/FDRMR-MEP can be summarized as follows: - Request and Response Message queues are made available via two "Fully decoupled Request/Response over AMQP" <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network) and another on the ground side (stacked with <Network binding> over the G/G Communication Network). These two bindings have to be instantiated according to the specific service (refer to the "contract" field) and directly accessed by SWIM enabled applications depending

	on the role (requestor, responder). - Airborne and Ground <Service binding> message queues are federated via "Request/Response over AMQP federation" <Internal service binding> (stacked with <Network binding> over the A/G Communication Network) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding has to be instantiated according to routing and segregation needs documented for each service (refer to TS §4.2.2.2.1). This requirement concerns the bindings of <Service binding> type for FDRR-MEP/FDRMR-MEP and it has been defined in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. In particular protocol stack, security, QoS, contract and binding relationships binding sections are described. In the Purple Profile TS §4.2.2.5 the same binding is described in a table form. The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding. Furthermore, it is anticipated that not all the applicable requirements are traced/included (e.g. QoS over AMQP requirements, reliability, message screening, AMQP over TLS requirements, etc.): conformance to this binding is not strictly covered only by the traced requirements.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Service binding>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b

<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0100
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0105
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0150
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0190
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0195
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0205
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0210
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0215
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0220
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0025
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055

[REQ]

Identifier	REQ-17.01-TS-0600.0240
Title	Request/Response over AMQP federation binding
Requirement	Request and Response message distribution federation shall be provided over the Request/Response over AMQP federation binding characterized as follows: + Protocol stack: - Stacking: Request/Response Messaging Entities Purple Profile messaging functionalities over AMQP 1.0 core over TLS {1.2 | 1.3} in the amqps form over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides request and response messages distribution for the federated FDRR-MEP and FDRMR-MEP. - Operations: AMQP 1.0 connection, session and link are initiated by the AMQP peer (i.e. Air SWIM Node) using an instance of this binding. Sending request or response message: . Sender entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with “source” link type (link type on the MQ side is “target”). Receiving request or response message: . Receiver entity establishes an AMQP 1.0 link with the request (response) MQ made available by this binding with “target” link type (link type on the MQ side is “source”). - Message structure& format: the AMQP 1.0 annotated message consists of the following sections used in accordance with the Purple Profile specification: . header, properties, application-data and footer from federated Fully decoupled Request/Response over AMQP binding instance. . one message-annotations section in case on-the-fly compression is enabled/provided. - Fault/failure/error: in accordance with AMQP 1.0 core. - Constraints: same as for Fully decoupled Request/Response over AMQP binding. + Security: - Authentication: . Point to point: mutual transport level authentication of AMQP 1.0 peers (Air and ground SWIM Nodes) through TLS {1.2|1.3} according to the amqps form only. . End to end: the binding provides mechanisms to transfer message level security

	information from the sender and the intended recipient(s). - Authorization: . Point to point: the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the access to the messaging resources made available through the binding. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Integrity: . Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Confidentiality: . Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. . End to end: the binding provides mechanisms to transfer message level security information from the sender and the intended recipient(s). - Non-repudiation: . Point to point: audit logging. . End to end: depending on the message level security controls used by the specific service. + QoS: - Delivery guarantees: the binding provides At-Most-Once. Optionally, it provides { At-Most-Once | At-Least-Once | Exactly-Once} delivery guarantees in accordance with Purple Profile design and constraints. AMQP peer (i.e. Air SWIM Node) ”connecting” (AMQP connection, session, link) to the instance of this binding should implement reconnection and retry policy as defined by the Purple Profile. - Lifetime: message with specified lifespan and Non-Temporary Queue. - Durability: when not constrained by the chosen delivery guarantee, {durable | non-durable} messages, and {non-durable | volatile | durable} message queues are supported. - Ordering guarantees: {FIFO | Best effort message priority} message ordering guarantees are provided. - CoSs: the instantiation of this binding allows to assign a specific class of service. + Contract:

	- Addressing: the binding does not constrain nor standardize the AMQP 1.0 core addressing scheme(s). Addressing scheme has to be documented together with non-opaque addressing for request and response message queues. - Messaging resources: message queues lifecycle is managed via administrative interfaces. The instantiation of this binding requires the creation and configuration of message queues. - Messaging Policies: messaging policies are managed via administrative interfaces. The instantiation of this binding requires the applicable messaging policies defined by the Purple Profile are documented and configured. Routing policies are mandatory to enable federation. - Security Policies: security policies are managed via administrative interfaces. The instantiation of this binding requires the security policies defined by the Purple Profile are documented and configured. - QoSs: the instantiation of this binding requires that the applicable QoSs are documented and configured taking into account QoSs of federated Fully decoupled Request/Response over AMQP binding instances. - CoS: the instantiation of this binding requires that the applicable CoS is documented and configured taking into account CoS of the federated Fully decoupled Request/Response over AMQP binding instances. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding> over the A/G Communication Network. - Federates Fully decoupled Request/Response over AMQP binding <Service binding>: the binding provides messaging functionalities aiming at federating Fully decoupled Request/Response over AMQP binding <Service binding> bindings pair(s). - (optionally) Relies on CDP and/or OCSP bindings: the binding optionally relies on (use with “consumer” role) CDP or/and OCSP for X.509v3 for certificate revocation status check.
Status	<validated>
Rationale	In accordance with Purple Profile technical viewpoint, Purple Profile enabled SWIM services are made accessible to the application layer (Purple Profile enabled SWIM applications) via a pair of bindings of type <Service binding> federated via a binding of type <Internal service binding>. In particular, the bindings triad for Purple Profile enabled SWIM service over FDRR-MEP/FDRMR-MEP can be summarized as follows: - Request and Response Message queues are made available via two “Fully decoupled Request/Response over AMQP” <Service binding>, one on the aircraft side (stacked with <Network binding> over the Aircraft Information Network) and another on the ground side (stacked with <Network binding> over the G/G Communication Network). These two bindings have to be instantiated according to the specific service (refer to the “contract” field) and directly accessed by SWIM enabled applications depending on the role (requestor, responder). - Airborne and Ground <Service binding> message queues are federated via

Company General Use

	"Request/Response over AMQP federation" <Internal service binding> (stacked with <Network binding> over the A/G Communication Network) provided by the Ground SWIM node and consumed by the Aircraft SWIM Node. This binding has to be instantiated according to routing and segregation needs documented for each service (refer to TS §4.2.2.2.1). This requirement concerns the bindings of <Internal service binding> type for FDRR-MEP/FDRMR-MEP and it has been defined in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. In particular protocol stack, security, QoS, contract and binding relationships binding sections are described. In the Purple Profile TS §4.2.2.5 the same binding is described in a table form. The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding. Furthermore, it is anticipated that not all the applicable requirements are traced/included (e.g. QoS over AMQP requirements, reliability, message screening, AMQP over TLS requirements, etc.): conformance to this binding is not strictly covered only by the traced requirements.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider>
Roles	<Responder><Requestor>
Selfstanding set	<Internal service binding>
Testability	<Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

<ALLOCATED_TO>	<Function>	Message Distribution Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0100
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0105
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0140
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0150
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0190
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0195
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0205
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0210
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0215
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0600.0220
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0135
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0160
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0180
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0185
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0165
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0170
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0175
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0025

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0020.0045
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055

4.3.7.2 CA/PKI Interface requirements and bindings

[REQ]

Identifier	REQ-17.01-TS-0440.0050
Title	HTTP 1.1 RFC 7230 interoperability standard
Requirement	The SWIM Node shall support IETF RFC 7230 Hypertext Transfer Protocol (HTTP/1.1), June 2014 https://tools.ietf.org/html/rfc7230.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. HTTP is used when accessing OCSP responder for X.509v3 certificate revocation status check and also for HTTP based CRL distribution point.
Category	<Interoperability><Interface>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0055
Title	HTTP over TLS interoperability standard
Requirement	The SWIM Node shall support IETF informational RFC 2818 HTTP Over TLS May 2000 http://tools.ietf.org/html/rfc2818.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. HTTPs is used when accessing OCSP responder for X.509v3 certificate revocation status check.
Category	<Interoperability><Interface>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0085
Title	OCSP Interoperability standard
Requirement	The SWIM Node shall support IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP) June 2013 http://tools.ietf.org/html/rfc6960.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.

	OCSP is used for online X.509v3 certificate revocation status check. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security><Interface>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0090
Title	LDAPv3 interoperability standard
Requirement	The SWIM Node shall support IETF RFC 4510 Proposed Standard, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006 http://www.rfc-editor.org/rfc/rfc4510.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. LDAPv3 is used for LDAP based CRL distribution point. This requirement covers NIST security control IA-4 (6).
Category	<Interoperability><Security><Interface>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>

Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0100
Title	LDAP Schema Definitions for X.509 Certificates interoperability standard
Requirement	The SWIM Node shall support IETF RFC 4523 Proposed Standard, Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates, June 2006 http://www.rfc-editor.org/rfc/rfc4523.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. LDAPv3 is used for LDAP based CRL distribution point. This requirement covers NIST security control IA-4 (6).
Category	<Interoperability><Security><Interface>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier

<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0105
Title	Public Key Infrastructure: Certification Path Building interoperability standard
Requirement	The SWIM Node shall support IETF RFC 4158 Internet X.509 Public Key Infrastructure: Certification Path Building September 2005 http://tools.ietf.org/html/rfc4158.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security><Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple profile

[REQ]

Identifier	REQ-17.01-TS-0440.0140
Title	Public Key Infrastructure Time-Stamp Protocol (TSP) interoperability standard
Requirement	The SWIM Node shall support IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) August 2001 http://www.rfc-editor.org/rfc/rfc3161.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. X.509v3 certificate is the digital identity used for mutual authentication and authorization. This requirement covers NIST security control AU-8.
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0145
Title	CMS Interoperability standard
Requirement	The SWIM Node shall support IETF RFC 5652 Internet Standard, Cryptographic Message Syntax (CMS), September 2009 http://www.rfc-editor.org/rfc/rfc5652.txt.
Status	<validated>

Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-8 (1).
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0155
Title	PKCS #12 Personal Information Exchange Syntax interoperability standard
Requirement	The SWIM Node shall support IETF RFC 7292 Internet Standard, PKCS #12 Personal Information Exchange Syntax v1.1, July 2014 https://tools.ietf.org/html/rfc7292.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. X.509v3 certificate is the digital identity used for mutual authentication and authorization. This requirement covers NIST security control IA-5 (2.b).
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>

Point of View	<ATM service><SWIM-TI provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0095
Title	Internet PKI Certificate and CRL Profile interoperability standard
Requirement	The SWIM Node shall support IETF RFC 5280 Proposed Standard, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 http://www.rfc-editor.org/rfc/rfc5280.txt.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. X.509v3 certificate is the digital identity used for mutual authentication and authorization. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0800.0100
Title	Internet X.509 Public Key Infrastructure Operational Protocols FTP and HTTP
Requirement	The SWIM Node shall support IETF RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols FTP and HTTP, May 1999 https://tools.ietf.org/html/rfc2585.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This standard concerns HTTP based CRL distribution point.
Category	<Interoperability><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management consumer>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0800.0105
Title	OCSP over HTTP(s) over TCP interface binding.
Requirement	OCSP services shall be provided over the binding characterized as follows: + Protocol stack: - Stacking: OCSP over HTTP 1.1 over TLS {1.2 | 1.3} over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides synchronous request/response MEP (SRR-MEP). - Operations: in accordance with OCSP standard. - Message structure& format: in accordance with OCSP standard. - Fault/failure/error: the service shall be able to determine the content of the HTTP status code and HTTP reason phrase. - Constraints: none. + Security: - Authentication: . Point to point: optionally server only or mutual transport level authentication through TLS {1.2|1.3}. - Authorization: . Point to point: optionally the digital identity authenticated at transport level (i.e. X.509v3 certificate) is used to authorize the OCSP requestor. - Integrity: . Point to point: OSCP responses are signed with OCSP responder's public key. When TLS is used the binding provides transport level integrity through TLS {1.2|1.3}. - Confidentiality: . Point to point: when TLS is used, the binding provides transport level confidentiality through TLS {1.2|1.3}. - Non-repudiation: . Point to point: audit logging. + QoS: none. + Contract: - Addressing: OCSP responder URL(s) replacing/complementing URL(s) included in the

	X.509v3 certificate (if any). - Any additional security information/configuration needed to enable the OCSP requestor to interact with the OCSP responder. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding>.
Status	<validated>
Rationale	The X.509v3 certificate revocation check is usually performed by: - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or - Consuming OCSP (Online Certificate Status Protocol) service(s), or - Combining both CRL and OCSP based certification revocation status mechanisms. In the Purple Profile the basic (<PP Core>) option for checking X.509 certificate revocation status is to rely on locally stored CRLs. The capability of Purple Profile enabled applications and SWIM Nodes to use OCSP based revocation status check is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts). OCSP services are used by Purple Profile enabled applications, Air SWIM Node and Ground SWIM Node through standard based interface bindings conformant with IETF RFC 6960. In particular OCSP over HTTP as described in the IETF RFC 6960 Appendix A is used and specified in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. OCSP based operations do not necessarily need security. Security can be applied but can lead to significant recursive complexity (RFC 6960 requires that OSCP responses are signed). This is why the binding allows message level (OCSP layer on top of HTTP) and transport level (HTTP over TLS) as valid options to authenticate the OCSP responder. This binding allows optionally to have mutual authentication at transport level (HTTP over TLS) in case it is required to authenticate the clients due to specific deployment options/security policies. If the OCSP server does not require some sort of authorization, an attacker can get the server to respond to arbitrary requests. Such responses may give the attacker information that may be valuable for a future attack. Furthermore, when required, the binding allows to apply the other security controls at transport level (HTTP over TLS). Authenticity at transport level has not to be confused with HTTP Basic and Digest Access Authentication that are not supported by this binding . The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows:

	- minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding.
Category	<Interface><Security>
Profile Part	<PP Air Security+><PP Ground Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<External service binding>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Enabler>	SWIM-SUPT-03a
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0055
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0085
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0105
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0140
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0300
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0305
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0310

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0270.0315

[REQ]

Identifier	REQ-17.01-TS-0800.0110
Title	CDP HTTP over TCP Interface Binding.
Requirement	HTTP CDP shall be provided over the binding characterized as follows: + Protocol stack: - Stacking: HTTP 1.1 GET over TCP over {IPv4 | IPv6}. - MEPs: the binding natively provides synchronous request/response MEP (SRR-MEP). - Operations: HTTP GET for retrieving the CRL file. - Message structure& format: in accordance with the standard. - Fault/failure/error: the service shall be able to determine the content of the HTTP status code and HTTP reason phrase. - Constraints: none. + Security: - Authentication: . None. - Authorization: . None. - Integrity: . Point to point: message level for CRL file. - Confidentiality: . None. - Non-repudiation: . None. + QoS: none. + Contract: - Addressing: HTTP CDP URL(s) replacing/complementing URL(s) included in the X.509v3 certificate (if any). - CRL issuer's X.509v3 certificate used to verify the signed CRL files.

	+ Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding>.
Status	<validated>
Rationale	The X.509v3 certificate revocation check is usually performed by: - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or - Consuming OCSP (Online Certificate Status Protocol) service(s), or - Combining both CRL and OCSP based certification revocation status mechanisms. In the Purple Profile the basic (<PP Core>) option for checking X.509 certificate revocation status is to rely on locally stored CRLs. CRLs are periodically issued by the CAs and typically installed/updated locally as part of maintenance activities. However, the CRLs expire and an expired CRL represents a possible vulnerability. When it is not possible to update on-the-fly the expired CRL, the revocation status check will fail. A standard mechanism allowing the retrieving of CRLs is the CRL distribution point (CDP). CAs typically provide online CDPs over HTTP (HTTP CDP) and/or over LDAP (LDAP CDP) and the endpoint addresses of these services could be also included in the certificates they issue. Basic (<PP Core>) Purple Profile option is based on a scheduled maintenance process ensuring that CRL are updated before they expire. The capability of Purple Profile enabled applications and SWIM Nodes to use HTTP CDPs and/or LDAP CDPs is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts). This requirement concerns HTTP based CDPs and it has been specified in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. The binding provides only the security control needed to ensure authenticity and integrity of the CRL file(s). The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding.
Category	<Interface><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>

Company General Use

Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<External service binding>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Enabler>	SWIM-SUPT-03a
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0050
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0055
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0105
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0140
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0095
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0800.0100
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050

[REQ]

Identifier	REQ-17.01-TS-0800.0115
Title	CDP LDAP over TLS over TCP Interface Binding.
Requirement	LDAP CDP shall be provided over the binding characterized as follows: + Protocol stack: - Stacking: LDAP v3 over TCP over TLS {1.2 | 1.3} over {IPv4 | IPv6}. - MEPs: the binding natively provides synchronous request/response MEP (SRR-MEP).

	- Operations: as defined per LDAP standard. - Message structure& format: in accordance with the LDAP standard. - Fault/failure/error: in accordance with the LDAP standard. - Constraints: none. + Security: - Authentication: . Point to point: server only or mutual transport level authentication through TLS {1.2|1.3} or LDAP Simple or SASL. - Authorization: . Point to point: server only or mutual transport level authentication through TLS {1.2|1.3} or LDAP Simple or SASL. - Integrity: . Point to point: the binding provides transport level integrity through TLS {1.2|1.3}. - Confidentiality: . Point to point: the binding provides transport level confidentiality through TLS {1.2|1.3}. - Non-repudiation: + QoS: none. + Contract: - Any addressing and security information needed to access LDAP CDP. + Binding relationships: - Stacked with <Network binding>: binding instances are stacked with {IPv4 | IPv6} <Network binding>.
Status	<validated>
Rationale	The X.509v3 certificate revocation check is usually performed by: - Checking if the certificate is included in the Certificates Revocation List (CRL) that is a resource available locally, or - Consuming OCSP (Online Certificate Status Protocol) service(s), or - Combining both CRL and OCSP based certification revocation status mechanisms. In the Purple Profile the basic (<PP Core>) option for checking X.509 certificate revocation status is to rely on locally stored CRLs. CRLs are periodically issued by the

	CAs and typically installed/updated locally as part of maintenance activities. However, the CRLs expire and an expired CRL represents a possible vulnerability. When it is not possible to update on-the-fly the expired CRL, the revocation status check will fail. A standard mechanism allowing the retrieving of CRLs is the CRL distribution point (CDP). CAs typically provide online CDPs over HTTP (HTTP CDP) and/or over LDAP (LDAP CDP) and the endpoint addresses of these services could be also included in the certificates they issue. Basic (<PP Core>) Purple Profile option is based on a scheduled maintenance process ensuring that CRL are updated before they expire. The capability of Purple Profile enabled applications and SWIM Nodes to use HTTP CDPs and/or LDAP CDPs is considered an advanced featured (<PP Air Security+> and <PP Ground Security+> profile parts). This requirement concerns LDAP based CDPs and it has been specified in accordance with Purple Profile technical viewpoint (TS §4.2.2) and interface bindings template documented in the Purple Profile TS. The binding allows different options for authentication and authorization. The first option is to rely on authentication and authorization mechanism at transport level (i.e. TLS). The second option is to use LDAP Simple mechanism defined in the LDAP standard. The third option is to use SASL (Simply Authentication and Security Layer). In LDAP based exchanges, External, Digest-MD5 and Kerberos V5 SASL mechanisms are typically used. The requirement includes (via <INCLUDES> links) additional requirements concerning messaging and security. Conformance to this interface binding requirement has to be evaluated as follows: - minimum: all the mandatory requirements belonging to mandatory profile parts and included by the binding. - advanced: in addition to the above, all the mandatory requirements belonging to optional profile parts and included by the binding.
Category	<Interface><Security>
Profile Part	<PP Ground Security+><PP Air Security+>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<External service binding>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Enabler>	SWIM-SUPT-03a
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0090
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0100
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0105
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0140
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0145
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0155
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0095
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0055
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0050

4.3.7.3 Network Interface requirements and bindings

[REQ]

Identifier	REQ-17.01-TS-0440.0015
Title	IPv4 RFC 791 interoperability standard
Requirement	The SWIM Node should support IETF RFC 791 Internet Protocol September 1981 http://tools.ietf.org/html/rfc791.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. Support for the IPv4 standard is mandatory for the Ground SWIM Node. Support for IPv4 for the Air SWIM Node is optional and it will not be supported at the same time as IPv6. Current aircraft support IPv4 in accordance with ARINC 821. It is expected that in the future aircraft will replace IPv4 with IPv6.
Category	<Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider><Network provider>

Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0020
Title	IPv6 RFC 8200 interoperability standard
Requirement	The SWIM Node shall support IETF RFC 8200 Internet Protocol, Version 6 (IPv6) Specification July 2017 http://tools.ietf.org/html/rfc8200.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. Support for the IPv6 standard is mandatory for the Ground SWIM Node. Support for IPv6 for the Air SWIM Node is optional and it will not be supported at the same time as IPv4. Current aircraft support IPv4 in accordance with ARINC 821. It is foreseen that in the future aircraft will replace IPv4 with IPv6.
Category	<Interoperability>
Profile Part	<PP Ground><PP Air Advanced>
Domain of Interest	<ICD>
Point of View	<ATM service><SWIM-TI provider><Network provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0025
Title	Interoperability standard. Requirements for Internet Hosts -- Communication Layers
Requirement	The SWIM Node shall support IETF RFC 1122 Internet Standard, Requirements for Internet Hosts Communication Layers, October 1989 http://tools.ietf.org/html/rfc1122.
Status	<validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c

<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0015
Title	Communication Network Infrastructure IP routing support
Requirement	The Communication Network Infrastructure shall provide IP routing.
Status	<in progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN).Taking into account the overall context and the large number of interconnected systems generally belonging to several different IP networks the support of IP routing at network level is needed.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0020
Title	Communication Network Infrastructure TCP support
Requirement	The Communication Network Infrastructure shall allow to use Transmission Control Protocol (RFC 793).
Status	<in progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN).Taking into account the overall context and the large number of interconnected systems which need to exchange information in efficient and reliable manner, the support of TCP protocol at network level is needed. All the network bindings specified require TCP/IP unicast. This requirement is applicable to all the three networks parts of the PP architecture. This requirement is applicable to all the three networks part of the PP architecture.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0030

Title	MTU, TCP buffer size
Requirement	The Communication Network infrastructure MTU max available shall be documented.
Status	<in progress>
Rationale	Throughput is dependent of the communication means (SATCOM, WIFI, CELLULAR, …) but is it also dependent of latency and TCP configuration (i.e. TCP windows size).MTU max is imposed by network infrastructure along the path between sender and receiver (TCP layer).The PP will certainly constrain the TCP buffer size and it shall be verified that MTU <=MTU max and TCP buffer size will be compatible with SWIM operation.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0100
Title	Air/Ground IP fragmentation
Requirement	The Air/Ground Network Infrastructure should support IP fragmentation/reassembly of IPv4 data as specified in IETF RFC 791 to maximise bandwidth usage.
Status	<in progress>

Rationale	IP fragmentation is an IPv4 process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<Network provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0120
Title	Interoperability standard. Internet Standard Subnetting Procedure
Requirement	The Communication Network infrastructure shall support IETF RFC 950, Internet Standard, Internet Standard Subnetting Procedure, August 1985 http://tools.ietf.org/html/rfc950.
Status	<in progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. There is no need for subnetting onboard current aircraft. In the future, as the aircraft networking complexity increases then it may be required.
Category	<Interoperability>
Profile Part	<PP Ground><PP Air Advanced>

Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0010
Title	Communication Network Infrastructure IPv4 support
Requirement	The Communication Network Infrastructure should provide IPv4 (RFC 791) support.
Status	<in progress>
Rationale	Support for the IPv4 standard is mandatory for the Air/Ground and Ground/Ground Communication Infrastructures. Support for IPv4 for the Aircraft information network is optional and it will not be supported at the same time as IPv6. Current aircraft support IPv4 in accordance with ARINC 821. It is expected that in the future aircraft will replace IPv4 with IPv6. The IP version/network binding will be configured as part of the configuration of service and internal bindings.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0005
Title	Communication Network Infrastructure IPv6 support
Requirement	The Communication Network Infrastructure shall provide IPv6 (RFC 8200) support.
Status	<in progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN).Taking into account the overall context, the large number of interconnected systems, performance and Quality of Service (QoS) the adoption of IPv6 at network level is needed. Support for the IPv6 standard is mandatory for the Air/Ground and Ground/Ground Communication Infrastructures. Support for IPv6 for Aircraft information network is optional and it will not be supported at the same time as IPv4. Current aircraft support IPv4 in accordance with ARINC 821. It is foreseen that in the future aircraft will replace IPv4 with IPv6. Support for IPv4 or IPv6 does not need to be the same for each network for end-to-end communications. The IP version will be configured as part of the configuration of service and internal bindings.
Category	<Interface>
Profile Part	<PP Ground><PP Air Advanced>

Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0440.0110
Title	IPv6 Node Requirements interoperability standard
Requirement	The Network infrastructure shall support IETF RFC 6434, Memo, IPv6 Node Requirements, December 2011 http://tools.ietf.org/html/rfc6434.
Status	<in progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. Reference to this specification assumes that all IPv6 nodes meet the minimum requirements specified in it.
Category	<Interoperability>
Profile Part	<PP Ground><PP Air Advanced>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Responder><Requestor><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0105
Title	Aircraft Information Network IPv6 support
Requirement	The Aircraft Information Network shall provide IPv6 (RFC 8200) support in accordance with AEEC 664 Part 3.
Status	<in progress>
Rationale	Support for IPv6 for the Aircraft information network is optional and it will not be supported at the same time as IPv4. Current aircraft support IPv4 in accordance with ARINC 821. In the future, it is expected that aircraft will replace IPv4 with IPv6. ARINC 664P3 Table 3.4.1-1 Internet Layer Requirements – Protocol Implementation Conformance Statement (RFC-1122 Paragraph 3.5) is applicable to both IPv4 and IPv6. Table 3.4.3-1 – IPv6 Extension Headers (RFC-2460 Paragraph 4.0) is applicable for IPv6. Gaps in A664 are identified in A686-d2: "Roadmap for IPv6 Transition in Aviation".
Category	<Interface>
Profile Part	<PP Air Advanced>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0110
Title	Aircraft network ADIF interface
Requirement	The Aircraft Information Network should allow Air SWIM Nodes to retrieve avionics parameters via a TCP/IP based ARINC 834 ADIF Interface.
Status	<validated>
Rationale	ARINC Specification 834 defines a set of protocols and services for the exchange of aircraft avionics data across aircraft networks.
Category	<Interface>
Profile Part	<PP Air>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0115
Title	Aircraft network segregation
Requirement	The Aircraft Information Network shall support the segregation of data in the AISD from other aircraft domains.
Status	<validated>
Rationale	ARINC Specification 664 defines the aircraft domains. Firewalls and other security mechanisms can be used to control the allowed communications.
Category	<Interface>
Profile Part	<PP Air>
Domain of Interest	<ICD>
Point of View	<Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0120
Title	Air/Ground data segregation
Requirement	The Air/Ground Network Infrastructure shall support the segregation of uplink/downlink data to and from the AISD from data from other aircraft domains.
Status	<validated>

Company General Use

Rationale	The Air/ground infrastructure needs to maintain the segregation of data over the air/ground link. This may be implemented as for AeroMACS by having separate ports on the datalink radio.
Category	<Interface>
Profile Part	<PP Air>
Domain of Interest	<ICD>
Point of View	<Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0040
Title	Communication Network Infrastructure network traffic classification (Class of services) support
Requirement	The Communication Network Infrastructure shall provide network traffic classification (Class of services) mechanisms for handling QoS at network level.
Status	<in progress>
Rationale	There is a need to put different priorities to differentiate high priority data flow to low priority data flow. The number of priority level shall be confirmed (high, medium, low ?) The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN).In order to optimize the use of network resources and to differentiate the priorities of PP level messages/traffic the network infrastructure has to support network traffic classification (Class of services) mechanisms. The precise levels/classes and classification mechanisms (layer 2, 3, or 4) are out of

	scope of this solution. They have to be identified and specified by solutions dealing with network layer.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0045
Title	Air/Ground Network Infrastructure CoSs
Requirement	The Air/Ground Network Infrastructure should provide at least two levels of CoSs: one level with guarantee of service (no congestion) and another with service best effort.
Status	<in progress>
Rationale	It can be anticipated that for certain applications a QoS will be necessary to prioritize messages. Deterministic behaviour of SWIM is expected but there are airspaces and A/C architectures for which it may not be possible to guarantee the service.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>

Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile

[REQ]

Identifier	REQ-17.01-TS-0490.0050
Title	IP Unicast IPv4
Requirement	Network Technical Interface should be instantiated according to the following binding: + IP Unicast IPv4 (32 bits) + Mapping IP to IP + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none.
Status	<validated>
Rationale	Basic Unicast IPv4 binding is mandatory for:

	- A/G Communication Network Infrastructure, which is an IP-based network used to interconnect the air SWIM Node with the ground SWIM Node. - G/G Communication Network Infrastructure(s), which is an IP-based network used to interconnect the ground SWIM Node with the ground SWIM-enabled ATM Applications. The Aircraft information network is used to interconnect aircraft AISD SWIM-enabled applications and air SWIM Nodes. Support for IPv4 for the Air SWIM Node is optional and it will not be supported at the same time as IPv6. Current aircraft support IPv4 in accordance with ARINC 821. It is expected that in the future aircraft will replace IPv4 with IPv6. The IP version/network binding will be configured as part of the configuration of service and internal bindings.
Category	<Interface>
Profile Part	<PP Core>
Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0490.0010
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0025
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0020

<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0030
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0120
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0040

[REQ]

Identifier	REQ-17.01-TS-0490.0055
Title	IP Unicast IPv6
Requirement	Network Technical Interface shall be instantiated according to the following binding: + IP Unicast IPv6 (128 bits) + Mapping IP to IP + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none.
Status	<validated>
Rationale	Basic Unicast IPv6 binding is mandatory for: - A/G Communication Network Infrastructure, which is an IP-based network used to interconnect the air SWIM Node with the ground SWIM Node. - G/G Communication Network Infrastructure(s), which is an IP-based network used to interconnect the ground SWIM Node and ground SWIM-enabled ATM Applications. The Aircraft information network is used to interconnect aircraft AISD SWIM-enabled applications and the Air SWIM Node. IPv6 will not be supported at the same time as IPv4. Current aircraft support IPv4 in accordance with ARINC 821. It is expected that in the future aircraft will replace IPv4 with IPv6. The IP version/network binding will be configured as part of the configuration of service and internal bindings.
Category	<Interface>
Profile Part	<PP Ground><PP Air Advanced>

Domain of Interest	<ICD>
Point of View	<SWIM-TI provider><Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile
<SATISFIES>	<ATMS Requirement>	REQ-17.01-TS-0490.0005
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0025
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0015
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0020
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0030
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0440.0120
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0110
<INCLUDES>	<ATMS Requirement>	REQ-17.01-TS-0490.0040

[REQ]

Identifier	REQ-17.01-TS-0490.0125
Title	SWIM Security Application Message Integrity Ensuring
Requirement	Application level messages integrity shall be ensured during all processing at Communications Network Infrastructure level.
Status	<in progress>
Rationale	The network shall maintain the integrity of the data when forwarding data over the

	network.
Category	<Security><Design>
Profile Part	<PP Core>
Domain of Interest	<ICD><Function/Behaviour>
Point of View	<Network provider>
Roles	<Requestor><Responder><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier
<ALLOCATED_TO>	<SESAR Solution>	PJ.17-01
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06b
<ALLOCATED_TO>	<Enabler>	SWIM-INFR-06c
<ALLOCATED_TO>	<Functional block>	SWIM Messaging Purple Profile
<ALLOCATED_TO>	<Functional block>	SWIM Security Purple Profile

5 Implementation Options

The identified implementation options concerning the Purple Profile are documented as part of the deployment viewpoint in §4.2.3. Main options concerns avionics installation options and cardinality of the relationship between the Air PP SWIM Node and Ground PP SWIM Node.

6 Assumptions

This chapter provides the main assumptions on which the Purple Profile TS has been defined.

Identifier	Description
PJ.17-01-ASSUMPTION.01	In the context of PJ.17-01, transformation/bridging capability has been further discussed and the decision is that in the PJ.17-01 TS the "bridging" capabilities related to the adaptation towards ground Profiles (Yellow, Blue, Green, etc.) will not be specified. This is mainly to avoid coupling between SWIM Profiles and because of the complexity of a complete bridging for all the existing interface bindings. This decision introduces following assumptions: - Ground provided services of interest for the aircraft are provided over Purple Profile <Service binding> options specified in this technical specification. - Ground provided services of interest for both the aircraft and ground systems are provided over multiple SWIM Profiles (Purple Profile for aircraft and whatever colour for other ground consumers). This requires that such bridging/transformations are implemented on the service provider side (no restrictions are provided in this TS on the what, how and how good).
PJ.17-01-ASSUMPTION.02	It is assumed that the CAs will be able to provide all the three bindings (LDAP CDP, HTTP CDP and OSCP).
PJ.17-01-ASSUMPTION.03	The Purple Profile messaging design includes handling of messages (not related to security purposes) based on identifiers for producer, consumer, service, etc. It is assumed that when moving to the SESAR deployment phase, a governed registry will be available to register applications, services, etc.
PJ.17-01-ASSUMPTION.04	Service specific message properties are assumed to be documented as part of the SWIM services design description.
PJ.17-01-ASSUMPTION.05	It is assumed that the technical design of a given PP enabled SWIM Service is built on one or more of the technical use cases identified in PP TS.

Table 75: PJ.17-01 TRL4 TS assumptions

7 References and Applicable Documents

7.1 Applicable Documents

Content Integration

[1] B.04.01 D138 EATMA Guidance Material

[2] EATMA Community pages

[3] SESAR ATM Lexicon

Content Development

[4] B4.2 D106 Transition Concept of Operations SESAR 2020

System and Service Development

[5] 08.01.01 D52: SWIM Foundation v2

[6] 08.01.01 D49: SWIM Compliance Criteria

[7] 08.01.03 D47: AIRM v4.1.0

[8] 08.03.10 D45: ISRM Foundation v00.08.00

[9] B.04.03 D102 SESAR Working Method on Services

[10] B.04.03 D128 ADD SESAR1

[11] B.04.05 Common Service Foundation Method

Performance Management

[12] B.04.01 D108 SESAR 2020 Transition Performance Framework

[13] B.04.01 D42 SESAR2020 Transition Validation

[14] B.05 D86 Guidance on KPIs and Data Collection support to SESAR 2020 transition.

[15] 16.06.06-D68 Part 1 –SESAR Cost Benefit Analysis – Integrated Model

[16] 16.06.06-D51-SESAR_1 Business Case Consolidated_Deliverable-00.01.00 and CBA

[17] Method to assess cost of European ATM improvements and technologies, EUROCONTROL (2014)

[18] ATM Cost Breakdown Structure_ed02_2014

[19] Standard Inputs for EUROCONTROL Cost Benefit Analyses

[20]16.06.06_D26-08 ATM CBA Quality Checklist

[21]16.06.06_D26_04_Guidelines_for_Producing_Benefit_and_Impact_Mechanisms

Validation

[22]03.00 D16 WP3 Engineering methodology

[23]Transition VALS SESAR 2020 - Consolidated deliverable with contribution from Operational Federating Projects

[24]European Operational Concept Validation Methodology (E-OCVM) - 3.0 [February 2010]

System Engineering

[25] SESAR 2020 Requirements and Validation Guidelines

Safety

[26]SESAR, Safety Reference Material, Edition 4.0, April 2016

[27]SESAR, Guidance to Apply the Safety Reference Material, Edition 3.0, April 2016

[28]SESAR, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015

[29]SESAR, Resilience Engineering Guidance, May 2016

Human Performance

[30]16.06.05 D 27 HP Reference Material D27

[31]16.04.02 D04 e-HP Repository - Release note

Environment Assessment

[32]SESAR, Environment Reference Material, alias, “Environmental impact assessment as part of the global SESAR validation”, Project 16.06.03, Deliverable D26, 2014.

[33]ICAO CAEP – “Guidance on Environmental Assessment of Proposed Air Traffic Management Operational Changes” document, Doc 10031.

Security

[34]16.06.02 D103 SESAR Security Ref Material Level

[35]16.06.02 D137 Minimum Set of Security Controls (MSSCs).

[36]16.06.02 D131 Security Database Application (CTRL_S)

7.2 Reference Documents

[37] ED-151 Operational Services and Environment Definition (OSED) for Aeronautical Information Services (AIS) and Meteorological (MET) Data Link Services, December 2007.

[38] PJ.17-01 D2.1.410, PJ.17-01 TRL4 Technical Specification, 00.02.00, May 2018.

[39] PJ.17-01 D2.1.440, PJ.17-01 TRL4 Technical validation activities report, 00.01.00, June 2018.

[40] ED-175 Safety and Performance Requirements (SPR) for AERONAUTICAL INFORMATION SERVICES (AIS) and METEOROLOGICAL (MET) DATA LINK SERVICES, January 2011.

[41] AMC 20-25 Airworthiness and operational consideration for Electronic Flight Bags (EFBs), ED Decision 2014/001/R.

[42] ARINC REPORT 660B CNS/ATM AVIONICS ARCHITECTURES SUPPORTING NEXTGEN/SESAR CONCEPTS, January 10, 2014.

[43] ARINC REPORT 821 AIRCRAFT NETWORK SERVER SYSTEM (NSS) FUNCTIONAL DEFINITION, December 9, 2008.

[44] ARINC CHARACTERISTIC 763-2 NETWORK SERVER SYSTEM, NOVEMBER 21, 2001.

[45] ARINC SPECIFICATION 834-7 AIRCRAFT DATA INTERFACE FUNCTION (ADIF), August 9, 2017

[46] ARINC REPORT 811 COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK, December 20, 2005.

[47] ARINC REPORT 852 GUIDANCE FOR SECURITY EVENT LOGGING IN AN IP ENVIRONMENT, June 21, 2017.

[48] ARINC REPORT 842-1 GUIDANCE FOR USAGE OF DIGITAL CERTIFICATES, December 12, 2013.

[49] ARINC SPECIFICATION 823P2 DATALINK SECURITY PART 2 – KEY MANAGEMENT, March 10, 2008.

[50] WMO AMDAR Observing System, http://www.wmo.int/pages/prog/www/GOS/ABO/AMDAR/About.html.

[51] SESAR 1 P14.01.03-D30, SWIM Architectural Definition Final (TAD).

[52] SESAR 1 P14.01.03 D39, “SWIM Profiles Final”, edition 00.01.01, 15/07/2016.

[53] SESAR 1 P14.01.04 D44-002, “SWIM-TI Identity Management Requirements”, edition 00.01.00, July 2016.

[54] Internet Engineering Task Force (IETF), Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, January 2010.

[55] W3C Recommendation XML Encryption Syntax and Processing 10 December 2002 http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

[56] W3C Recommendation XML Signature Syntax and Processing (Second Edition) 10 June 2008 http://www.w3.org/TR/xmldsig-core/.

[57] PJ.17-01 Messaging characterization, January 2019.

[58] PJ.17-01 D2.3.640, PJ.17-01 Technical Validation Report TRL6, 00.01.00, November 2019.

[59] Aircraft Access to SWIM (AAtS) Concept of Operations (ConOps), July 31, 2013.

[60] Aircraft Access to SWIM Implementation Guidance Document, Version 2.0, 3/1/2013.

[61] Aircraft Access to SWIM Full Data Exchange Technical Concept Paper, Version 1.0, 7/31/2013.

Appendix A Purple Profile SWIM Profile Assertion (SPA)

This appendix provides the Purple Profile SPA [52]. The SWIM Purple Profile scope and structure are detailed in the following sections.

The table below provides a summary of this SWIM profile scope and key elements.

Profile Name	Scope	Key elements
Purple Profile	▪ High latency and/or low bandwidth conditions. ▪ No Real-time or near real-time uses. ▪ Need to minimize the communication overhead and transport connections number. ▪ Technical solution as much as possible supported out-of-the-box. ▪ To enable proper information sharing in scenarios where availability of end-to-end connectivity over the communication infrastructure is intermittent and unpredictable. ▪ Air/Ground ATM information exchanges.	▪ Purple Profile consists of different parts: <PP Core>, <PP Air>, <PP Ground>, <PP Air Security+>, <PP Ground Security+>, <PP Air Advanced> and <PP Air Advanced>. ▪ Advanced Message Queuing Protocol (AMQP) (version 1.0). ▪ Transport level security controls (TLS 1.2 and TLS 1.3). ▪ Cryptography (PKI X.509 v3, XML Encryption, XML Signature and ECRYPT II).

Table 76: Purple Profile scope and key elements

A.1 Scope

Some types of information sharing in ATM are performed in challenging conditions and/or constraints and need specific infrastructure.

The PP is explicitly targeted at:

- High latency constraints and/or low bandwidth conditions;
- Need to minimize the communication overhead and the number of transport connections due to high cost of use of the communication;
- Intermittent and unpredictable availability of end-to-end connectivity over the communication infrastructure;
- Facilitate Security controls through constraints in the interaction patterns;
- Permanent need for time, space and synchronization decoupling between participants (asynchronous operations)
- Simple and easily certifiable information producers and consumers

The PP is explicitly not targeted at:

- Real time services
- Synchronisation coupling between participants (synchronous operations)

The PP favours consistency above availability in the context of Brewer's CAP theorem.

A.2 Rationale

The PP is not the result of any prior legacy activity on Profiles. It has emerged as a solution for requirements and constraints for information sharing between airborne and ground systems.

This context presents a combination of challenges that are not easily or adequately solved by established SWIM-TI technology.

Challenge: **available bandwidth is limited**

- Verbose protocols and/or inefficient data formats could lead to several forms of starvation whereby some messages might never reach the intended destination(s) or whereby delays would be accumulated, continuously increasing and leading to congestion. Waste of bandwidth is not acceptable over costly aeronautical data links (e.g. SATCOM).
    - The prominent selection of textual XML data format by the SESAR programme can be questioned since it is very verbose and is not efficient from a bandwidth perspective.
    - This issue can be dealt with by applying the SWIM-TI data re-encoding (i.e. data transformation) and/or compression techniques. For some data formats, data format transformation can be more efficient than data compressing. For instance, the data encoding using the ASN.1/PER bit-oriented encoding rules results in a significantly smaller message size than a compressed form of the same data keeping textual XML data format.
- The effect of the constraint on bandwidth is exacerbated by the high cost of the communications. Any overhead generated by the data format and by the communication protocols needs to be minimized.

Challenge: **an Aircraft can go out of network coverage**

- Any form of communication that requires the participants to be present in the communication at the same time will suffer and fail. Some form of store-forward mechanism is required whereby a message that is sent by a participant in a communication between Aircraft and Ground, is stored without the need for the sender to know whether the other targeted participant(s) are currently connected or not, so to allow later forwarding to the other participant(s) at a time the other participant(s) can connect.
- The established SWIM-TI technology can meet such requirements to some extent but cannot provide out of the box the level of time decoupling that is required. For some forms of the SWIM-TI technology (typically the Publish/Subscribe Push model and the Synchronous Request/Reply model), the required time decoupling functionality could only be provided through significant/complementary additional application developments which are entirely proprietary.
- A middleware technology model that has a high suitability for provision of time decoupling between participants is based on Message Queuing (MQ).

- The current release of the PP defines the SWIM Wire Interface using an open and free MQ protocol: the AMQP (Advanced Message Queuing Protocol), which is based on a binary data flow via TCP.

Challenge: **need for space and synchronization decoupling**

- It must be possible to communicate messages with participants without knowing the precise identity (who) of the recipient or recipients (how many) and to exchange a message between participants without the need for any of the participants to block its activity until an answer is returned.
- The established SWIM-TI technology can meet such requirements through the Publish/Subscribe MEPs. However for most of the established SWIM-TI technology, either the technical requirements are not feasible in a communication between Aircraft and Ground or a solution will not be able to provide sufficient QoS or a solution will hit other constraints that are specific in the Aircraft - Ground communication.
    - As the Aircraft may connect over a wide range of access networks, it is not realistic to assume that IP Multicast and VPN services will be supported in each of them.
    - Incompatibility with the specific security needs as documented below.
    - The reliable delivery of a message cannot be guaranteed.
- There is a need for a MEP that would be a combination of 2 correlated point-to-point patterns (Message queuing and Request/Reply) to form a kind of Fully Decoupled Request/Reply (refer to SWIM-TI TAD):
    - This MEP does not map natively to the existing SWIM-TI Messaging Technologies.
    - This MEP can be emulated by one or more other MEPs provided by the existing SWIM-TI technology. However:
        - doing so would introduce significant complexity and cost compared to the technology that provides or supports the MEP natively.
        - such emulation is not a common way of using the messaging technology and when done can raise undesired side-effects and difficulties.
        - COTS providers do not actively advocate or promote such capabilities.

Challenge: **specific security needs**

- The allowed data exchanges with the ground systems must be in the category of information requests from the EFB/PED Type A as defined in EASA AMC 20-25 for non-safety critical airborne operations.
- Due to security reasons, ground-initiated communications to aircraft are forbidden. This means that the setup of a TCP session must always be initiated by the aircraft to prevent attacks from the ground.
- UDP-based communication is easier to hijack and more vulnerable to spoofing than TCP. Hence the use of the UDP protocol is precluded.

- The Aircraft also needs to filter out data content and to check the validity of uplink messages. The PP enables to make it easily and to minimize number of exchange checks.

Challenge: **the airborne information producers/consumers need to be simple**

- Certified airborne software is very costly: the design of the airborne information producers/consumers and communication protocols needs to be as simple as possible to reduce their development and certification costs.

A.3 Structure

The PP is not the result of any prior legacy activity on Profiles. It has emerged as a solution for requirements and constraints for information sharing between airborne and ground systems.

This context presents a combination of challenges that are not easily or adequately solved by established SWIM-TI technology.

A.3.1 Interoperability

- The messaging protocol:

  The PP is not targeted to be firmly bound to a particular messaging protocol in particular:

  - The current release of the profile performs messaging on a Message queuing.
  - The current release of the profile includes both message queuing technology independent and message queuing technology specific models for the SWIM Wire interfaces; this maximize the reusability of the specification in case a different messaging technology is used at wire level.
  - The current release of the profile defines the SWIM Wire Interface using AMQP version 1.0.
  - The Advanced Message Queuing Protocol (AMQP) is an open internet protocol for business messaging. It defines a binary wire-level protocol that allows for the reliable exchange of business messages between two parties. AMQP has a layered architecture and the specification is organized as a set of parts that reflects that architecture. Part 1 defines the AMQP type system and encoding. Part 2 defines the AMQP transport layer, an efficient, binary, peer-to-peer protocol for transporting messages between two processes over a network. Part 3 defines the AMQP message format, with a concrete encoding. Part 4 defines how interactions can be grouped within atomic transactions. Part 5 defines the AMQP security layers.

- Security:

  The PP uses transport level security capabilities to provide most of its security controls such as confidentiality, integrity, authenticity. These controls are based on the TLS set of protocols which are at a high level of maturity and standardisation.

The PP uses specific constraints as additional security controls: a non-trivial and highly specific security element in the PP consists of the constraint that a TCP session can only be initiated from the Aircraft to the Ground. Despite this constraint, a bi-directional message flow at higher levels is required.

- Data format:
  Currently the PP uses MIME types including restrictions. These formats are highly standardised and are highly mature.

A.3.2 Reuse and size

The technology footprint of the PP is narrow and focused:

- There is only a single version of a messaging protocol.
- There are multiple data formats but they are known and common.

The messaging technology of the PP has capabilities that are not easily or adequately provided through other technologies. Wherever such capabilities are needed and sufficient, the PP can be reused.

A.3.3 Constraints, competing requirements and risks

The OASIS AMQP 1.0 standard specification has a significant potential considering the industries that support it but the potential still needs to be realised.

The Message queuing provided by AMQP is very well suited as a solution for the scope of the PP. There are alternative products that also provide queue-based messaging: they are wide-spread, successful and categorised under the term MOM (Message Oriented Middleware). However these MOM products are typically based on proprietary protocols only and are therefore out of scope. From open standards perspective there are hardly any alternatives to AMQP.

A.3.4 Modular structure

As detailed in A.3.6 several profile parts [52] have been identified for the Purple Profile. The defined modular structure aims:

- at identifying requirements applicable to both aircraft and ground side PP.
- at separating mandatory from optional requirements
- at separating requirements applicable only to aircraft side PP from requirements applicable only to ground side PP.

A.3.5 Lifecycle of the SWIM Profile

The queue-based messaging concept is very mature. The concept is actively used since 1983.

The Advanced Message Queuing Protocol (AMQP) aims to provide interoperability between the various queue-based messaging solutions through a standardized wire-protocol.

The PKI concept is very mature. However the PKI processes for the Aircraft are not standardized, so every vendor or airline may implement own processes.

Moreover, it is expected that some security algorithms may get broken or updated, so the set of cryptographic algorithms or even the key length is expected to change.

From a FR and NFR point of view, many specifications have been issued in a Bottom-Up manner and have not yet been confirmed by Top-Down specifications. There is a high probability that FR and/or NFR of the PP will change.

The current version of the PP is defined in support of strategic information sharing (e.g. AIS/MET services defined by RTCA SC-206). It is foreseen that in the future the PP will have to be defined in support of more tactical services (AOC AIS/MET for avionic systems).

At very long term safety services could also be envisaged in relation with ATC.

A.3.6 Design rules

There is no conflict of the scope of the PP with the design rules described in SWIM Profile definition §5.2.4 [52].

A.3.7 Design criteria

In order

- identify requirements applicable to both aircraft and ground side PP.
- distinguish mandatory from optional requirements
- distinguish requirements applicable only to aircraft side PP from requirements applicable only to ground side PP.

several profile parts have been identified for the Purple Profile . In particular the following design criteria have been applied:

- All mandatory shall/should/may functional and non-functional requirements applicable to both aircraft and ground PP have been allocated to a profile part (<PP Core>) mandatory for both ground and aircraft PP.
- All mandatory shall/should/may functional and non-functional requirements applicable to ground PP have been allocated to a profile part (<PP Ground>) mandatory for ground PP.
- All mandatory shall/should/may functional and non-functional requirements applicable to aircraft PP have been allocated to a profile part (<PP Air>) mandatory for aircraft PP.
- Optional ground and aircraft specific profile parts have been identified for advanced requirements such as security, performance, etc.

The semantics of each profile part is described in A.3.8.

A.3.8 Recommended structure

The PP structure is depicted in Figure 45.

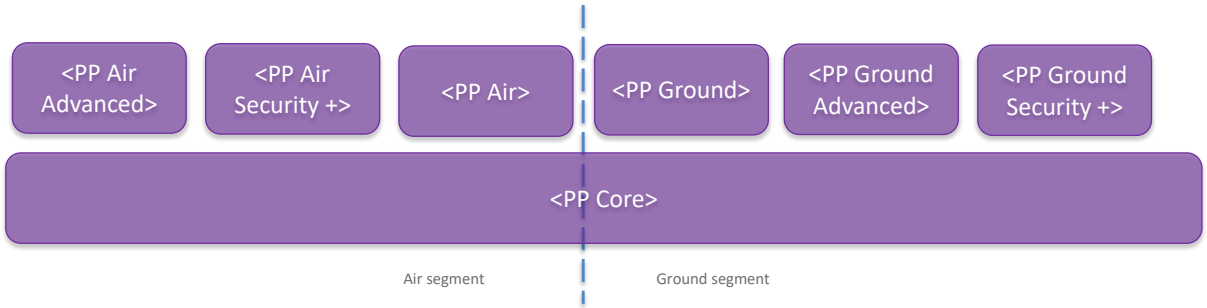


Figure 45: Purple Profile Profile Parts design

<PP Core>:

- Mandatory profile part that may include shall/should/may REQs.
- It includes REQs applicable to both aircraft and ground PP. Being a core profile part it is mandatory for both ground and aircraft PP.
- This part includes REQs of different type including messaging, «basic» security and bindings.

<PP Ground>:

- It includes REQs applicable ONLY to ground. It is (conformance statement) mandatory only for ground PP.
- This part may include shall/should/may REQs.
- This part includes REQs of different type including messaging, «basic» security, bindings, etc.
- Method of composition:
- - <Stacked> relationship with <PP Core>.
- - <SidebySide> relationship with <PP Air> (are independent but must be composed to realize the PP).

<PP Air>:

- It includes REQs applicable ONLY to aircraft. It is (conformance statement) mandatory only for aircraft PP.
- This part may include shall/should/may REQs.
- This part includes REQs of different type including messaging, «basic» security, bindings, etc.
- Method of composition:
    - <Stacked> relationship with <PP Core>.
    - <SidebySide> relationship with <PP Ground> (are independent but must be composed to realize the PP).

<PP Ground Security+>:

- It includes REQs applicable ONLY to ground. It is (conformance statement) optional for ground PP.
- This part may include shall/should/may REQs.
- This part includes advanced functional and non-functional security REQs.
- Scope:
  - Advance functional security REQs (e.g. policy management).
  - Advance non-functional security REQs (e.g. advance security controls, strictness on regulations, security patching).
- Method of composition:
  - <Stacked> relationship with <PP Core>.
  - <SidebySide> relationship with all the <PP Ground*> parts.
  - <SidebySide> relationship with all the <PP Air*> parts.

<PP Air Security+>:

- It includes REQs applicable ONLY to aircraft. It is (conformance statement) optional for aircraft PP.
- This part may include shall/should/may REQs.
- This part includes advanced functional and non-functional security REQs.
- Scope:
  - Advance functional security REQs (e.g. policy management).
  - Advance non-functional security REQs (e.g. advance security controls, strictness on regulations, security patching).
- Method of composition:
  - <Stacked> relationship with <PP Core>.
  - <SidebySide> relationship with all the <PP Air*> parts.
  - <SidebySide> relationship with all the <PP Ground*> parts.

<PP Ground Advanced>:

- It includes REQs applicable ONLY to ground. It is (conformance statement) optional for ground PP.
- This part may include shall/should/may REQs.
- This part includes REQs of different type including messaging, «basic» security, bindings, etc.
- Scope:

- Advance NFRs such as availability, performances, etc.
- Advance Functional Requirements.

- Method of composition:
  - <Stacked> relationship with <PP Core>.
  - <SidebySide> relationship with all the <PP Ground*> parts.
  - <SidebySide> relationship with all the <PP Air*> parts.

<PP Air Advanced>:

- It includes REQs applicable ONLY to aircraft. It is (conformance statement) optional for aircraft PP.
- This part may include shall/should/may REQs.
- This part includes REQs of different type including messaging, «basic» security, bindings, etc.
- Scope:
  - Advance NFRs such as availability, performances, etc.
  - Advance Functional Requirements.
- Method of composition:
  - <Stacked> relationship with <PP Core>.
  - <SidebySide> relationship with all the <PP Air*> parts.
  - <SidebySide> relationship with all the <PP Ground*> parts.

A.4 Conformance Statements

This section provides conformance statements applicable to the PP. It is important to take into account that for all the conformance statements, the <ATMS Requirement> linked element types described in §C.3.1 apply. In particular the requirements set related to a given conformance statement has to be built applying also <ATMS Requirement> linked element types.

Furthermore, the conformance statements refer to roles and profile parts described respectively in §C.2.4 and §C.2.1.

Title	Purple Profile Full Conformance
Conformance statement	A conforming implementation for any role and any profile part shall cover at least all the mandatory requirements expressed in all the profile parts.
Rationale	A conforming implementation claiming for Purple Profile full conformance must implement at least all the SHALLs requirements irrespective of the roles and profile parts.

Title	Purple Profile Profile Part Conformance
Conformance statement	A conforming implementation for a given profile part and for any role shall cover at least all the mandatory requirements expressed in the applicable profile part.
Rationale	A conforming implementation claiming for Purple Profile <Profile Part> (e.g. <PP Core>, <PP Air>, etc.) conformance must implement at least all the SHALLs requirements traced to that profile part irrespective of the roles.

Title	Purple Profile Role Conformance
Conformance statement	A conforming implementation for a given role shall cover at least all the mandatory requirements traced to that role.
Rationale	A conforming implementation claiming for Purple Profile <Role> (e.g. <Subscription handler>, <Requestor>, etc.) conformance must implement at least all the SHALLs requirements traced to that role irrespective of the profile parts.

Title	Purple Profile Role and Profile Part Conformance
Conformance statement	A conforming implementation for a given role and profile part shall cover at least all the mandatory requirements expressed in that profile part which are traced to that role.
Rationale	A conforming implementation claiming for Purple Profile <Role> (e.g. <Subscription handler>, <Requestor>, etc.) and <Profile Part> (e.g. <PP Core>, <PP Air>, etc.) conformance must implement at least all the SHALLs requirements from that profile part which are traced to that role.

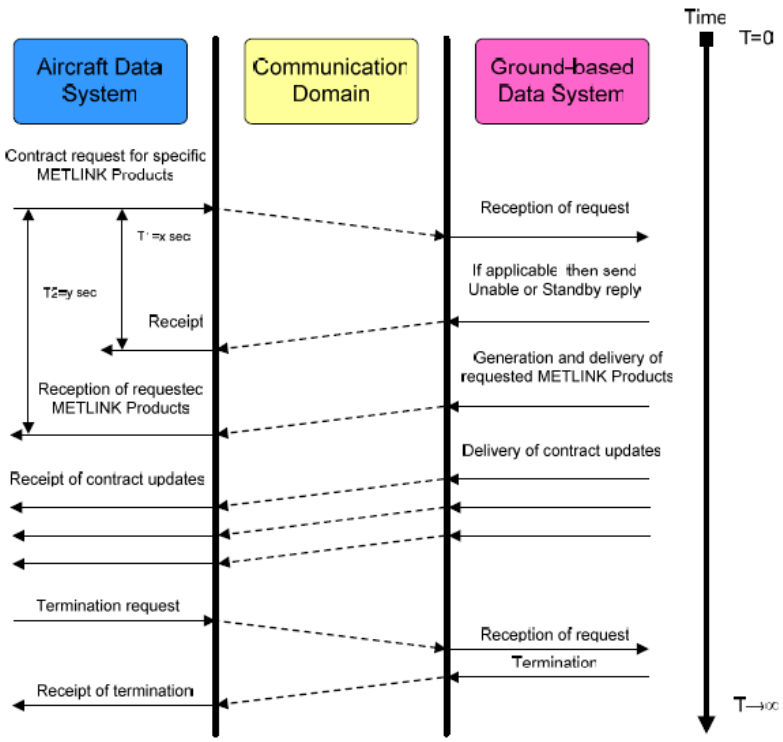
Appendix B MEPs and Messaging characterization

This appendix provides the PJ.17-01 defined characterization of entities, events and characteristics concerning information exchange based on Message Queues and Message Topics. It provides also the definition of the FDRMR-MEP as extension of the SWIM-TI MEPs catalogue from the SWIM-TI TAD [51].

B.1 FDRMR-MEP definition

The FDRMR-MEP has been identified starting from the end to end behaviour described for the contract datalink mode in the ED-151 [37]. As described in the figure below (the source is the ED-151), the contract datalink mode includes two main aspects not covered by the FDRR-MEP [51]:

- Following a request from the requestor, the responder responds with multiple responses.
- The requestor may explicitly request to the responder to terminate the sending of response messages triggered by the initial request.



Source: ED-151

Figure 46: ED-151 Contract datalink mode end to end behaviour

The FDRMR-MEP has the same characteristics of the FDRR-MEP. Here below the SWIM-TI TAD MEP characterization table (Table 6 in [51]) is provided by extending it with the FDRMR-MEP characteristics:

MEP	Direction conversation	Cardinality	Time Decoupling		Synchronization Decoupling		Space Decoupling	
	Consumer=C Provider=P Subscriber=S Publisher=Pu		Consumer / Subscriber	Provider / Publisher	Consumer / Subscriber	Provider / Publisher	Consumer / Subscriber	Provider / Publisher
Synchronous Request/Reply (SRR-MEP)	2 way (C-> P > C)	1-1	No	No	No	Yes	No	No
Asynchronous Request/Reply (ARR-MEP)	2 way (C-> P > C)	1-1	No	No	Yes	Yes	No	No
Observer Push (OPUSH-MEP)	1 way (Pu -> S)	1-many	No	No	Yes	Yes	No	No
Observer Pull (OPULL-MEP)	1 way (Pu -> S) Synchronous R/R	1-many	No	No	Yes	Yes	No	No
Publish/Subscribe Push (PSPUSH-MEP)	1 way (Pu -> S)	many-many	Yes	Yes	Yes	Yes	Yes	Yes
Publish/Subscribe Pull (PSPULL-MEP)	1 way (Pu -> S) Synchronous R/R	many-many	Yes	Yes	Yes	Yes	Yes	Yes
Asynchronous Fire & Forget (AFF-MEP)	1 way (C -> P), 2 way (C-> P > C)	1-1	Yes	Yes	Yes	Yes	No	No
Fully Decoupled Request/Reply (FDRR-MEP)	2 way (C-> P > C)	1-1	Yes	Yes	Yes	Yes	Yes	Yes
Fully Decoupled Request/Multi-Reply (or Response) (FDRMR-MEP)	2 way (C-> P > C)	1-1	Yes	Yes	Yes	Yes	Yes	Yes

Table 77: Extended MEP characterization

In the remaining part of this appendix the FDRMR-MEP is described using similar approach used in the TAD for other MEPs.

B.1.1 Fully decoupled Request/Multi-Response MEP

A requestor sends a request message in the messaging service. The identity of the responder is unknown by the requestor. The messaging service attempts to send the request message to a responder. When the request reaches the responder, it receives the message at some undetermined time and processes the request. The responder sends periodically response to the messaging system which forwards it to the requestor. The responder terminates sending the responses according to information (e.g. duration) provided by the requestor (if any) or if the requestor explicitly sends a termination request. In the second case, the responder sends a termination response.

Both requestor and responder do not know each other. The requestor and responder do not have to be present at the same time. The requestor and responder are not blocked waiting on each other.

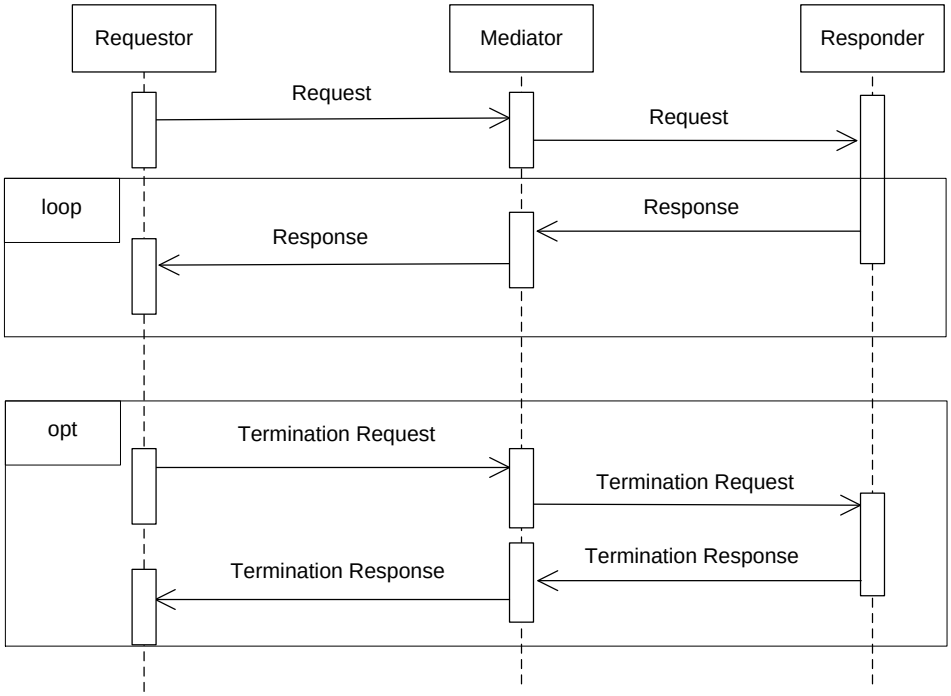


Figure 47: FDRMR-MEP Sequence diagram

B.2 Messaging characterization

In the context of the PJ.17-01 solution, the required architecture is described in a functional view that is technology agnostic. This functional view can be mapped to one or more technologies. A key element of this functional view, consists of the messaging functionality expressed in terms of Message Queue, Message Topic and Subscription.

There are no major global well-known standardisation entities that have created an exhaustive ontology/terminology for messaging. Many technology standards and products use their own localised ontologies/models. Further, at the time of mapping such ontology/characteristics to concrete technology there is a very high probably that this will create very significant confusion for

many Stakeholders because of the existing semantic non-alignment of existing standards and products.

Hence expression of the required functionality in a functional view is not trivial and requires a minimal development of an ontology that is shared for the purpose of PJ.17-01, i.e. establish only the functional characteristics that are relevant for PJ.17-01.

PJ.17-01 defined a messaging characterization [57] which complements the SESAR 1 TAD of WP14 where the main focus was on Message Exchange Patterns. The scope of the messaging characterization is not to repeat what was already defined in SESAR 1 but to reuse some of the concepts and extend the ontology for the purpose of unambiguous definitions of Message Queue, Message Topic and Subscription.

B.2.1 Statement of applicability to Purple Profile

This section aims at providing entities/events/characteristics SoA (statement of applicability) to Purple Profile. In particular for each entity/event/characteristic, the SoA is expected to provide values and rationale concerning following SoA fields:

- ***Applicability*** = *Applicable* or *Not Applicable*. This indicates if the entity/event/characteristic is applicable.
- (if *Applicability* = *Applicable*) ***Applicability level*** =
    - *Purple Profile* -> the entity/event/characteristic is applicable to both Aircraft/Air Purple Profile and Ground Purple Profile.
    - *Aircraft/Air Purple Profile* -> the entity/event/characteristic is applicable only to the Aircraft/Air Purple Profile.
    - *Ground Purple Profile* -> the entity/event/characteristic is applicable only to the Ground Purple Profile.
- (if *Applicability* = *Applicable*) ***Mandatoriness*** = *Mandatory* or *Optional*. For applicable entity/event/characteristic, this indicates if the derived functional requirements concern mandatory or optional functions.
- (if *Mandatoriness* = *Optional*) ***Mandatoriness level*** =
    - *Optional Profile part* -> all the requirements derived from the applicability of the entity/event/characteristic must be in a “shall” or “should” form.
    - *Mandatory Profile part* -> all the requirements derived from the applicability of the entity/event/characteristic must be in a “should” form.

Provided rationale should be enough detailed, clear and complete to justify the values and to support activities in the context of the technical view.

Per-Entity SoA

This section provides SoA of entities to Purple Profile.

Entity	Applicability	Applicability level	Rationale

Entity	Applicability	Applicability level	Rationale
Message	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile.
Message Queue	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile.
Sender	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile. In the Purple Profile functional view, this entity is a Purple Profile enabled application. This is true also in the Purple Profile technical view but in this case also the Air SWIM Node and the Ground SWIM Node are instances of this entity. This is linked to the technical view level realization of the applicable MEPs.
Receiver	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile. In the Purple Profile functional view, this entity is a Purple Profile enabled application. This is true also in the Purple Profile technical view but in this case also the Air SWIM Node and the Ground SWIM Node are instances of this entity. This is linked to the technical view level realization of the applicable MEPs. Purple Profile allows only exclusive receiver: a given

Company General Use

Entity	Applicability	Applicability level	Rationale
			Message Queue can be consumed by one and only one receiver.
Intermediary	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile. In the Purple Profile functional view, this entity is the Purple Profile. In the Purple Profile technical view this entity are the interconnected Air and Ground SWIM Nodes. This is linked to the technical view level realization of the applicable MEPs.
Message Topic	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile.
Publisher	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile. In the Purple Profile functional view, this entity is a Purple Profile enabled application. This is true also in the Purple Profile technical view but in this case also the Air SWIM Node and the Ground SWIM Node are instances of this entity. This is linked to the technical view level realization of the applicable MEPs.
Subscriber	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile.

Entity	Applicability	Applicability level	Rationale
			In both Purple Profile functional and technical views, this entity is a Purple Profile enabled application.
Subscription	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile.
Subscription handler	Applicable	Purple Profile	Basic entity needed to introduce and describe the Message Exchange Patterns (MEPs) applicable to the Purple Profile. For a given ground provided (uplink) Purple Profile enabled SWIM service, functions allocated to this entity could be provided by: - A given Ground SWIM Node on behalf of the SWIM service, or - Messaging capabilities on the SWIM service side. For air provided (downlink) Purple Profile enabled SWIM service, different options/policies concerning the allocation of this entity's functions could be identified. This mainly depends on the cardinality of the SWIM service endpoint of the ground and the aircraft. Typically the cardinality is 1-N meaning that ground applications subscribe to Message topic where publication messages from different aircraft are available. Proper federation logics between air and ground side Subscription handler function are needed. This is further detailed in the Purple Profile technical view

Company General Use

Entity	Applicability	Applicability level	Rationale
			but following options could apply: - The subscription request is accepted on the ground if all (or a given group of) the air side subscription handlers concerning that service accept the request. - The subscription request is processed and accepted on the ground on behalf of all the aircraft. The air side subscription handlers are notified about the active subscription. This allows A/G network resource optimization: messages are be downlinked only if at least one active subscription exists.

Table 78: per-entity SoA – applicability

Entity	Mandatoriness	Mandatoriness level	Rationale
Message	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Message Queue	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Sender	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Receiver	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.

Entity	Mandatoriness	Mandatoriness level	Rationale
Intermediary	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Message Topic	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Publisher	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Subscriber	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Subscription	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.
Subscription handler	Mandatory	N/A (it is not optional)	Being a basic entity for the description of the MEPs in the context of the Purple Profile, this entity is mandatory.

Table 79: per-entity SoA - mandatoriness

Per-Event SoA

This section provides SoA of events to Purple Profile.

Event	Applicability	Applicability level	Rationale
Connection establishment	Applicable	Purple Profile	In this characterization following connection pairs are identified: - Sender/Publisher -> Message Queue/Topic.

Event	Applicability	Applicability level	Rationale
			- Intermediary <- Receiver/Subscriber. In the Purple Profile functional and technical views the connection/disconnection/reconnection events have to be interpreted according to the mapping of these entities provided in the per-entity SoA section. Furthermore a list of alternate addresses to be used to connect/reconnect to should be configurable.
Connection establishment failure	Applicable	Purple Profile	As for Connection establishment event. Even if this event may concern different connections, its occurrences for Air SWIM Node -> Ground SWIM Node(s) connection(s) have to be properly assessed and handled when describing the Purple Profile technical view. Furthermore, in addition to considerations provided for the "Message not delivered" event, it should be evaluated the needs for monitoring functions able to distinguish between network (e.g. partitioning) and application (e.g. shutdown) failures.
Disconnection	Applicable	Purple Profile	As for Connection establishment event. Even if this event may concern different connections, its occurrences for Air SWIM Node -> Ground SWIM Node(s) connection(s) have to be properly assessed and handled when describing the Purple Profile technical view.
Abnormal disconnection	Applicable	Purple Profile	As for Connection establishment event. Even if this event may concern different connections, its occurrences for Air SWIM Node -> Ground SWIM Node(s) connection(s) have to be properly assessed and handled when describing the Purple Profile technical view. Furthermore, in addition to considerations provided for the "Message not delivered" event, it should be evaluated the needs for monitoring functions able to distinguish between network (e.g. partitioning) and application (e.g. shutdown) failures.

Event	Applicability	Applicability level	Rationale
Reconnection	Applicable	Purple Profile	As for Connection establishment event. Even if this event may concern different connections, its occurrences for Air SWIM Node -> Ground SWIM Node(s) connection(s) have to be properly assessed and handled when describing the Purple Profile technical view.
Reconnection establishment failure	Applicable	Purple Profile	As for Connection establishment event. Even if this event may concern different connections, its occurrences for Air SWIM Node -> Ground SWIM Node(s) connection(s) have to be properly assessed and handled when describing the Purple Profile technical view. Furthermore, in addition to considerations provided for the "Message not delivered" event, it should be evaluated the needs for monitoring functions able to distinguish between network (e.g. partitioning) and application (e.g. shutdown) failures.
Send a message (enqueue)	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Publish a message	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Subscription	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Filtering	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section. The Purple Profile provides two mechanisms to define filtering criteria: - Filtering policies allowing administrators to configure

Event	Applicability	Applicability level	Rationale
			(configuration time and optionally at run-time) filtering criteria for both queue and topic based information exchanges. - Filtering criteria provided by subscribers at subscription time (evaluated in AND relationships with any filtering policy). Currently it is not considered applicable (at least as core capability) to allow subscribers to update the filtering criteria after the subscription. In particular, currently in order to add/update filtering criteria the subscriber has to unsubscribe and then to subscribe again.
Delivery	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Receive a Message from a Message Queue	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Receive a Message from a Message Topic	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Unsubscription	Applicable	Purple Profile	In the Purple Profile functional and technical views this event has to be interpreted according to the mapping of the concerning entities provided in the per-entity SoA section.
Message expiration	Applicable	Purple Profile	In both Purple Profile functional and technical view context-based filtering and routing concerning expired messages have to be properly specified. In particular two main aspects have to be further detailed: - Routing policy: per service category or for specific service the policy should allow to configure at least the queue where the expired messages will be

Event	Applicability	Applicability level	Rationale
			routed, how long messages will be kept in the queue and what information will be logged about this event. - monitoring functions: it could be necessary to foreseen monitoring agents consuming specific events for reporting (e.g. dashboard). These agents may consume queue where expired messages are routed to ("dead letter queue").
Message not delivered	Applicable	Purple Profile	In both Purple Profile functional and technical view context-based filtering and routing concerning undelivered messages have to be properly specified. In addition to similar filtering/routing/monitoring considerations provided for the "Message expiration" event, for undelivered messages additional aspects should be detailed: - maximum number of retries should be configurable. - (linked to other events and to delivery guarantees) list of alternate addresses to be used to connect/reconnect to should be configurable. - delivery failure reason (e.g. network partition, maximum number of retries, etc.) should be reported together with event's severity.
Message dropped	Applicable	Purple Profile	In both Purple Profile functional and technical view, this event should be assessed and applicable design and requirements provided accordingly. Similar considerations/recommendations (e.g. monitoring) provided for Message expiration and Message not delivered events apply also to this event.

Table 80: per-event SoA – applicability

Event	Mandatoriness	Mandatoriness level	Rationale
Connection establishment	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Connection establishment failure	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account the fact that this event may occur. However, when details about some functions are available (design and specification phases) it should be evaluated if some of them could be "should" requirements or optional profile parts. In particular functions derived from monitoring needs could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Disconnection	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Abnormal disconnection	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account the fact that this event may occur. However, when details about some functions are available (design and specification phases) it should be evaluated if some of them could be "should" requirements or optional profile parts. In particular functions derived from monitoring needs could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Reconnection	**Optional**	Optional Profile part	Advanced functions that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile

Company General Use

Event	Mandatoriness	Mandatoriness level	Rationale
			parts. Its needs depend on the specific SWIM service NFRs. Furthermore it is strictly linked also to the supported delivery guarantees.
Reconnection establishment failure	**Optional**	Optional Profile part	As for the Reconnection event.
Send a message (enqueue)	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Publish a message	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Subscription	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Filtering	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Delivery	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Receive a Message from a Message Queue	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Receive a Message from a Message Topic	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.
Unsubscription	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account this event.

Company General Use

Event	Mandatoriness	Mandatoriness level	Rationale
Message expiration	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account the fact that this event may occur. However, when details about some functions are available (design and specification phases) it should be evaluated if some of them could be "should" requirements, optional profile parts or applicable to different profile parts distinguishing air and ground SWIM Nodes. For instance functions derived from monitoring needs could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Message not delivered	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account the fact that this event may occur. However, when details about some functions are available (design and specification phases) it should be evaluated if some of them could be "should" requirements or optional profile parts. For instance, functions derived from monitoring needs could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Message dropped	Mandatory	N/A (it is not optional)	It is mandatory to design and specify the Purple Profile taking into account the fact that this event may occur. However, when details about some functions are available (design and specification phases) it should be evaluated if some of them could be "should"

Company General Use

Event	Mandatoriness	Mandatoriness level	Rationale
			requirements, optional profile parts or applicable to different profile parts distinguishing air and ground SWIM Nodes. For instance, functions derived from monitoring needs could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.

Table 81: per-event SoA - mandatoriness

Per-Characteristic SoA

This section provides SoA of characteristics to Purple Profile.

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
Message lifespan/expiration	Message with zero/unspecified lifespan	**Not Applicable**	N/A (it is applicable)	In order to avoid message starvation in MQ and MT (resources saving) messages which will not expire are not allowed in the PP. This design decision is also coherent with the fact that advisory information (AI/MET) have typically a limited lifetime.
Message lifespan/expiration	Message with non-zero/specified lifespan	Applicable	Purple Profile	Basic message level characteristic useful in distributed messaging systems.
Message queue lifetime	Temporary Message Queue	**Not Applicable**	N/A (it is applicable)	There are no needs to allow this type of queue. Furthermore, the temporary queues may be also considered a possible security vulnerability. Finally, creation of messaging resources must be strictly

Company General Use

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				controlled by the administrator of the intermediary to prevent exhausting its resources.
Message queue lifetime	Non-Temporary Queue	Applicable	Purple Profile	The only kind of Message queue lifetime the Purple Profile supports.
Message topic lifetime	Temporary Message Topic	**Not Applicable**	N/A (it is applicable)	There are no needs to allow this type of topic. Furthermore, the temporary queues may be also considered a possible security vulnerability. Finally, creation of messaging resources must be strictly controlled by the administrator of the intermediary to prevent exhausting its resources.
Message topic lifetime	Non-Temporary Topic	Applicable	Purple Profile	The only kind of Message topic lifetime the Purple Profile supports.
Subscription lifetime	Subscription with zero/unspecified lifespan	Applicable	Purple Profile	This is a basic characteristic needed for the Publish/Subscribe MEP.
Subscription lifetime	Subscription with non-zero/specified lifespan	Applicable	Purple Profile	It is an advanced feature that could be useful for some specific services (protecting consumption of resources allocated to subscribers which do not unsubscribe) and/or subscribers. A cons is that the expiration time

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				provided by the subscriber could not be always fitting its needs (duration of the subscription) leading to the need to renew the subscription / subscribe again. The subscription "expiration" could be also linked to SWIM service/application level specific aspects such as the flight legs. The Purple Profile should allow this option via optional subscription policies.
Message Durability	Durable	Applicable	Purple Profile	Basic message level characteristic useful in messaging where different levels of delivery guarantees are supported.
Message Durability	Non-Durable	Applicable	Purple Profile	Basic message level characteristic useful in messaging where different levels of delivery guarantees are supported.
Message Queue Durability	Non-Durable	Applicable	Purple Profile	Basic message queue level characteristic in messaging systems.
Message Queue Durability	Volatile	Applicable	Purple Profile	Advanced message queue level characteristic in messaging systems considered applicable to specific services.
Message Queue Durability	Durable	Applicable	Purple Profile	Advanced message queue level characteristic in messaging systems

Company General Use

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				considered applicable to specific services.
Message Topic Durability	Non-Durable	Applicable	Purple Profile	Basic message topic level characteristic in messaging systems.
Message Topic Durability	Volatile	Applicable	Purple Profile	Advanced message topic level characteristic in messaging systems considered applicable to specific services.
Message Topic Durability	Durable	Applicable	Purple Profile	Advanced message topic level characteristic in messaging systems considered applicable to specific services.
Subscription Durability	Non-Durable	Applicable	Purple Profile **(Not allowed for aircraft application subscriptions)**	Basic subscription level characteristic in messaging systems.
Subscription Durability	Durable	Applicable	Purple Profile	Advanced subscription level characteristic in messaging systems considered applicable to specific services.
Subscription handler Durability	Non-Durable	**Not Applicable**	N/A (it is applicable)	Taking into account the key functions allocated to this entity, it is considered not acceptable that the Subscription handler might not survive a failure/restart of the intermediary.
Subscription handler Durability	Volatile	Applicable	Purple Profile	Advanced subscription handler level characteristic in messaging systems considered applicable

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				to specific services.
Subscription handler Durability	Durable	Applicable	Purple Profile **(recommended)**	Advanced subscription handler level characteristic in messaging systems considered applicable to specific services.
Message Priority	-	Applicable	Purple Profile	Basic message level characteristic useful in messaging systems.
Message Queue Ordering	FIFO	Applicable	Purple Profile	Basic message queue level characteristic useful in messaging systems.
Message Queue Ordering	Message Priority:strict	**Not Applicable**	N/A (it is applicable)	It is considered impossible/too complex to achieve.
Message Queue Ordering	Message Priority:best effort	Applicable	Purple Profile	The strict priority ordering is not required: best effort ordering is required meaning that realizations of this QoS should be stricter as possible. Several options could be identified at technical level. One could be to assign priority to Message queues each with FIFO ordering strategy in a way transparent to the sender and the receiver. In order to prevent starvation of messages in the low priority queue, the intermediary applies as sort of round-robin scheduling (this schema cannot ensure the strict

Company General Use

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				ordering). Depending on the assessment of the interoperability needs, in the technical view specific design solutions could specified or not.
Message Topic Ordering	FIFO	Applicable	Purple Profile	Basic message topic level characteristic useful in messaging systems.
Message Topic Ordering	Message Priority:strict	**Not Applicable**	N/A (it is applicable)	It is considered impossible/too complex to achieve.
Message Topic Ordering	Message Priority:best effort	Applicable	Purple Profile	The strict priority ordering is not required: best effort ordering is required meaning that realizations of this QoS should be stricter as possible. Several options could be identified at technical level. Depending on the assessment of the interoperability needs, in the technical view specific design solutions could specified or not.
Point-to-point delivery guarantees	At-Most-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs.
Point-to-point delivery guarantees	At-Least-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs.
Point-to-point delivery guarantees	Exactly-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs. This delivery

Company General Use

Characteristic	Characteristic value	Applicability	Applicability level	Rationale
				guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability.
Point-to-point delivery guarantees	No delivery guarantees	Applicable	Purple Profile **(Not allowed for air-ground connections)**	Applicable according to SWIM service FRs and NFRs.
End-to-end delivery guarantees	At-Most-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs.
End-to-end delivery guarantees	At-Least-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs.
End-to-end delivery guarantees	Exactly-Once	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs. This delivery guarantee is realized by combining At-Least-Once with message duplicates detection (message UUID) capability.
End-to-end delivery guarantees	No delivery guarantees	Applicable	Purple Profile	Applicable according to SWIM service FRs and NFRs.

Table 82: per-characteristic SoA - applicability

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
Message lifespan/expiration	Message with zero/unspecified lifespan	N/A (it is not applicable)	N/A (it is not applicable)	
Message lifespan/expiration	Message with non-zero/specified lifespan	Mandatory	N/A (it is not optional)	The only one Message lifespan/expiration supported.

Company General Use

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
Message queue lifetime	Temporary Message Queue	N/A (it is not applicable)	N/A (it is not applicable)	
Message queue lifetime	Non-Temporary Queue	Mandatory	N/A (it is not optional)	The only one Message queue lifetime supported.
Message topic lifetime	Temporary Message Topic	N/A (it is not applicable)	N/A (it is not applicable)	
Message topic lifetime	Non-Temporary Topic	Mandatory	N/A (it is not optional)	The only one Message topic lifetime supported.
Subscription lifetime	Subscription with zero/unspecified lifespan	Mandatory	N/A (it is not optional)	The only one Subscription lifetime supported.
Subscription lifetime	Subscription with non-zero/specified lifespan	**Optional**	Optional Profile part	Advanced capabilities that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Message Durability	Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support both durable and non-durable messages as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Message Durability	Non-Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support both durable and non-durable messages as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
				chosen.
Message Queue Durability	Non-Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message queue durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Message Queue Durability	Volatile	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message queue durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Message Queue Durability	Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message queue durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Message Topic Durability	Non-Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message topic durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
Message Topic Durability	Volatile	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message topic durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Message Topic Durability	Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support all the 3 message topic durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs the appropriate value is chosen.
Subscription Durability	Non-Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support the 2 subscription durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs and subscribing application needs, the appropriate value is chosen.
Subscription Durability	Durable	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support the 2 subscription durability levels as part of the core (and mandatory) functions. Depending on the SWIM services level NFRs and subscribing application needs, the appropriate value

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
				is chosen.
Subscription handler Durability	Non-Durable	N/A (it is not applicable)	N/A (it is not applicable)	
Subscription handler Durability	Volatile	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support at least subscription handler volatile durability level as part of the core (and mandatory) functions.
Subscription handler Durability	Durable	**Optional**	Optional Profile part	Advanced durability level that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts.
Message Priority	-	**Optional**	Optional Profile part	Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
Message Queue Ordering	FIFO	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support at least FIFO ordering as part of the core (and mandatory) functions.
Message Queue Ordering	Message Priority:strict	N/A (it is not applicable)	N/A (it is not applicable)	
Message Queue Ordering	Message Priority:best effort	**Optional**	Optional Profile part	Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
				parts. Its needs depend on the specific SWIM service NFRs.
Message Topic Ordering	FIFO	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support at least FIFO ordering as part of the core (and mandatory) functions.
Message Topic Ordering	Message Priority:strict	N/A (it is not applicable)	N/A (it is not applicable)	
Message Topic Ordering	Message Priority:best effort	**Optional**	Optional Profile part	Advanced ordering that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
Point-to-point delivery guarantees	At-Most-Once	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support this delivery guarantee level as part of the core (and mandatory) functions.
Point-to-point delivery guarantees	At-Least-Once	**Optional**	Optional Profile part	Advanced functions that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
Point-to-point delivery	Exactly-Once	**Optional**	Optional Profile part	Advanced functions that could be allocated to <PP

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
guarantees				Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
Point-to-point delivery guarantees	No delivery guarantees	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support this delivery guarantee level as part of the core (and mandatory) functions.
End-to-end delivery guarantees	At-Most-Once	Mandatory	N/A (it is not optional)	The Purple Profile is expected to support this delivery guarantee level as part of the core (and mandatory) functions.
End-to-end delivery guarantees	At-Least-Once	**Optional**	Optional Profile part	Advanced functions that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
End-to-end delivery guarantees	Exactly-Once	**Optional**	Optional Profile part	Advanced functions that could be allocated to <PP Ground Advanced> and/or <PP Air Advanced> profile parts. Its needs depend on the specific SWIM service NFRs.
End-to-end delivery	No delivery	Mandatory	N/A (it is not	The Purple Profile is expected to support

Characteristic	Characteristic value	Mandatoriness	Mandatoriness level	Rationale
guarantees	guarantees		optional)	this delivery guarantee level as part of the core (and mandatory) functions.

Table 83: per-characteristic SoA - mandatoriness

Appendix C PJ.17-01 requirements guidance

This appendix provides PJ.17-01 specific guidance about requirements complementing SESAR2020 programme level guidance.

C.1 Specific template for requirement text

For a number of specifications the requirement text follows a specific template in order to be able to express a coherent atomic view of a set of elements.

C.1.1 Interface Bindings

A number of specifications are related to the technical configuration of the Internal Interfaces and External Interfaces of the SWIM-TI. The key element of such technical configuration is the binding specification.

The requirement text of a binding specification is presented in a specific format as it has to bring and bind together a set of different specifications and present all these specifications as a single atomic requirement that applies in its whole. The structure of the requirement text documented below is applicable to all types of bindings.

In order to keep the requirement text of the binding readable and limited in size, a set of specifications which are part of the atomic concept, have not been included directly in the requirement text but they are referenced through the <INCLUDES> links of the binding. The effect of each <INCLUDES> link is equivalent to effective inclusion of the entire requirement text of the referenced specification in requirement text of the binding.

The requirement text of a binding identifies in distinct sections:

- Protocol stack: this section is composed by following sub-sections:
  - Stacking: this sub-section describes the details of particular grouping and linking of distinct protocols. In many cases, it suffices to describe the vertical layering from top to bottom.
  - MEPs: MEP(s) offered by the binding [Appendix B].
  - Operations: operations to interact (messaging) with the binding. For AMQP based bindings, this is based on the messaging characterization and its instantiation over AMQP 1.0 core.
  - Message structure & format: this sub-section identifies message structure, types, etc., and any applicable constraints.
  - Fault/failure/error: if applicable, this sub-section describes the extent to which one side of the interface controls the behaviour of the other side of the interface related to faults/exceptions in this binding.
  - Constraints: this sub-section describes per protocol in the protocol stack, the applicable constraints compared to the baseline. Typically such descriptions includes:
    - features of a protocol that are not required
    - features of a protocol that shall not be used
    - limitations on value ranges

The baseline:

- for any protocol in the protocol stack: the standards that describe the protocols.
- for linking/grouping/aggregation of protocols: the standards that describe such linking/grouping/aggregation of protocols.

- Security: this section describes in detail the security controls and their use. A protocol stack may include many distinct security controls that provide similar functionality and individual security controls may support distinct mechanisms and technologies. In such cases, it is necessary to explicitly describe each aspect of the available security controls. An explicit description for at least following list of security needs/security controls needs to be present in the SWIM-TI "binding" requirement.
- Quality of service (QoSs): this section describes QoS provided by SWIM-TI "binding" and that directly impact interoperability.
- Contract: this section identifies elements representing sort of parameters governing the instantiation of the binding for a specific SWIM service.
- Binding relationships: when applicable, this section identifies the direct relationships between the binding and other bindings of different type.

C.1.2 Measurements

In conformity with ISO/IEC 25010 and ISO/IEC 25023:

- A requirement related to Performance Efficiency (ISO/IEC 25010) shall, where applicable, be expressed in one or more measurements and the conditions whereunder these measurements are performed.

  A single requirement can contain multiple measurements and can contain only a single set of conditions. The set of conditions applies to all measurements. The measurements will specified first and followed by the conditions in a clearly separated manner.

  The measurements will be listed under a heading "Measurements".

  The conditions will be listed under a heading "Measurement conditions".
- A requirement related to Reliability (ISO/IEC 25010) shall, where applicable, be expressed in one or more measurements and the conditions whereunder these measurements are performed as well as for which period of time.
- A single requirement can contain multiple measurements and can contain only a single set of conditions and can contain only a single period of time. The measurements will specified first and followed by the conditions in a clearly separated manner and followed by the period of time in a clearly separated manner.

  The measurements will be listed under a heading "Measurements".

  The conditions will be listed under a heading "Measurement conditions".

  The period of time will be specified under a heading "Period of time".

C.2 SWIM-TI specific requirement attributes

This section includes the description and the semantic of requirement attributes/fields used in this technical specification documents. These attributes complement the SESAR programme guidelines.

The various forms of categorisation of the requirements through the attributes that are described below constitute an aid to enable to quickly find relevant requirements in a particular context. In some cases the categorisation is formal and complete, in some cases it is not.

The attributes types are meant to be strictly generic and applicable across all SWIM Profiles. The attribute values could contain values that are specific for a SWIM Profile, SWIM Profile Part, Role or Selfstanding Set.

Each of the attributes can be considered as a dimension on which filtering can be applied. Combined filtering on multiple distinct attributes is meant to be meaningful.

Following attributes are based on SWIM-TI ontology elements included in the SWIM-TI TAD [51] and SWIM Profiles definition [52].

C.2.1 “Profile Part" Attribute

Rationale

The notion of Profile Part is explained in the SWIM-TI Ontology. PP specific profile parts are described in §Appendix A.

Possible values

Each requirement is part of at least one Profile Part. Currently, one of more of the following values are allowed:

- <PP Core>
- <PP Ground>
- <PP Air>
- <PP Ground Security+>
- <PP Air Security+>
- <PP Ground Advanced>
- <PP Air Advanced>

Considerations

A Profile Part is used to group functionality into subsets ranging from minimal or core functionality to full or complete functionality. The difference with the notion of Level is that Profile Parts are not necessarily nested (called stacked pattern) but can also exist side-by-side.

The “Profile Part” is the encompassing and coordinating entity that ensures the coherent information sharing by all participants in a Plug & Play manner.

It suffices for a participant to stick to the specifications of a Profile Part in a conforming manner to be ensured of coherent information sharing with other participants in the context of the same Profile Part.

Profile Parts themselves can be composed in the different manners with other Profile Parts. This information is captured in both the SPA in dedicated requirements with category <Design>.

The currently defined methods of composition are one of

- <N/A>
- <Stacked>: the profile part inherits and specializes the profile part (requirements) on which it is stacked on.
- <SidebySide>: the profile part is independent of and can exist in any combination with one or more other parts.

C.2.2 "Domain of interest" Attribute

Rationale

The requirements in the Profiles range from Interoperability and Interface related requirements over SLA and Governance related requirements to system Behaviour and Functional related requirements. The relevance of the requirements is not always considered to be equal (hence the use of the term Domain of interest). The competencies to address such requirements are often not concentrated in a single person or single entity. There is a high level of decoupling between 4 domains of interest present in the Profiles including lifecycle.

Example:

Interoperability and interface related requirements are considered crucial and immutable while SLA and governance related requirements and system behaviour and functional related requirements are subjected to negotiations and changing methods of operation and organisation.

SLA and Governance related requirements can change over time at a different pace than Interoperability and Interface related requirements.

Possible values

One requirement can be of interest for more than one Domain of interest. One requirement can be applicable to more than one Profile Part.

Currently, one of more of the following values are allowed:

- <ICD>
- <SLA>
- <Governance>
- <Function/Behaviour>
- <Unspecified>

<Unspecified> is an indication of a problem that needs to be solved. If a requirement is not found to be needed for any of the 3 providers (defined in subsequent Point of View), then the relevance of the requirement may be questionable.

The interest of a Domain of interest for a requirement can be different depending on the Profile Part.

The list of values is not fixed. For instance: currently it is proposed to keep Function and Behaviour related requirements together in the same Domain of interest but they could be split into 2 distinct Domain of interest.

Considerations

There is no single common standardised definition of ICD. Requirements related to protocols and the configuration thereof inside the SWIM-TI that allow 2 or more parties to participate in an interaction are part of ICD.

Requirements related to the interaction between the SWIM-TI and external entities such as ATM specific services and the Network are part of an ICD.

The notion of SLA is covered by various standards (e.g. ITIL and ISO/IEC 20000, CMMI, COBIT) but there is no single common standardised definition of SLA. The notion of SLA as Domain of Interest represents a subset of the topics typically covered by the various standards:

Requirements related to qualitative and quantitative measurements are part of SLA.

The notion Governance is covered by various standards (e.g. ITIL, CMMI, various ISO IT Governance Frameworks) but there is no single common standardised definition of Governance.

Requirements related to configurability are part of Governance.

Requirement related to Roles and responsibilities are part of Governance.

Requirements related to the manner an implementation is operated and organised are part of Governance.

There is no single common standardised definition of Behaviour/Functional.

Most of the Domain of Interest can be constructed to some extent in a mechanical manner from an existing attribute Category and in such case would not need an additional attribute. Without change of the current definition of Category following represents the best possible mapping:

<ICD> = <Interoperability> + <Interface> + <HMI>

<SLA > = <Performance> + <Maintainability> +<Reliability> + <Safety> + <Security>

<Governance> = <Maintainability> +<Reliability> + <Safety> + <Security>

<Function/Behaviour> = <Functional>

Above use of category presents following restrictions:

- there is no way to select one or more specific requirements that have classified in one or more of the limited list of Categories, to some of the Domains of interest remaining semantically correct.
- (example) the requirements on configurability of policies are in the Domain of Interest <Governance> but they are tagged in the Category <Functional>. Getting such specifications in <Governance> with existing construct would require to tag in one of the Categories that are mapped to <SLA/Governance>. However none of them covers configurability of policies.

Because of these limitations, the existing attribute Category as is cannot be re-used. This is why a dedicated requirement attribute has been introduced.

C.2.3 "Point of view" Attribute

Rationale

From a system context diagram like perspective, the SWIM-TI interacts mainly with the ATM specific services and with the network. The providers for each of these 3 interacting entities have different needs regarding to which specifications of the SWIM-TI are relevant.

Example:

The service provider may not need to be aware of the requirement that states that HMAC shall be provided a Message Authentication Codes algorithm but must know about the Message Exchange Patterns (MEP) the SWIM-TI offers to an ATM specific service. The network provider may not need to be aware of the MEPs the SWIM-TI offers to an ATM specific service but needs to know which version of IGMP or MLD is required. The SWIM-TI provider will need to know all requirements.

Possible values

One requirement can be needed for more than one provider. One requirement can be applicable to more than one Profile Part.

Currently, one of more of the following values are allowed:

- <SWIM-TI provider>
- <ATM service>
- <Network provider>
- <Unspecified>

<Unspecified> is an indication of a problem that needs to be solved. If a requirement is not found to be needed for any of the 3 providers, then the relevance of the requirement may be questionable.

This list could be changed but is considered to be mature and stable: the likelihood of being changed is very low.

Considerations

At least some of the requirements can be allocated to a Point of view in a mechanical manner.

Examples:

- bindings of the Network bindings group can be allocated systematically to the <Network provider>.
- bindings of the Service bindings group can be allocated systematically to the <ATM service>.

The need of a provider for a requirement can be different depending on the Profile Part. This is theoretical and is not expected to occur often, nevertheless in case it would be needed then the possible values should also include the Profile Part which is not currently foreseen. In case such need would occur, it is to be considered as an anomaly and possibly requiring a requirement to be split.

C.2.4 "Role" Attribute

Rationale

The notion of role is explained in the SWIM-TI Ontology and applied in the SWIM Profiles definition. Furthermore is has been further refined as part of the PJ.17-01 messaging characterization (§Appendix B).

Possible values

One of more of the following:

- <Requestor>
- <Responder>
- <Subscriber>
- <Subscription handler>
- <Publisher>
- <Publication consumer>
- <Publication mediator>
- <Identity Management provider>
- <Identity Management consumer>
- <Shareable function provider>
- <Shareable function consumer>
- <Unspecified>

The interpretation is as follows:

- <Requestor>, <Responder>: roles in the Request/Response type of MEPs.
- <Subscriber>, <Subscription handler>, <Publisher>, <Publication consumer>, <Publication mediator>: roles in the Publish/Subscribe type of MEPs and Observer type of MEPs.
- <Identity Management Provider>,<Identity Management client>: roles in an Identity management context.
- <Shareable function provider>, <Shareable function consumer>: generic roles for shareable functions, if no specific role denomination is required (e.g. run-time registry sharable function).
- <Unspecified> is an indication of a problem that needs to be solved.

Considerations

Similar to above (Domain of Interest and Point of View), theoretically the role for a requirement can be different depending on the Profile Part. This is theoretical and is not expected to occur often, nevertheless in case it would be needed then the possible values should also include the Profile Part which is not currently foreseen. In case such need would occur, it is to be considered as an anomaly and possibly requiring a requirement to be split.

C.2.5 “Selfstanding set" Attribute

Rationale

The notion of Selfstanding Set is explained in the SWIM-TI Ontology Terminology Relationships and Semantics.

Possible values

Some requirements represent a Selfstanding Set of requirements. One of the following:

- <Service binding>
- <Network binding>
- <External service binding>
- <Internal service binding>
- <Not applicable>
- <Unspecified>

The interpretation is as follows:

<Service binding> : external to the SWIM-TI and related to an ATM specific service only.

<Network binding> : external to the SWIM-TI and related to the Network only.

<External service binding> : external to the SWIM-TI and not a <Service binding> or a <Network binding>.

<Internal service binding> : internal to the SWIM-TI only and related to any such internal service.

<Not applicable>: any specification that does not represent a Selfstanding Set.

<Unspecified> is an indication of a problem that needs to be solved.

Considerations

It should be possible starting from one requirement that represents an entire Selfstanding Set of requirements to mechanically identity and assemble all applicable requirements. The existing defined relationships such as <APPILIES TO> and <INCLUDES> should be used.

Such relationships can exist in multiple stages and will be identified as being part of the Selfstanding set. Example:

REQ X is the requirement that represents a Selfstanding set of requirements.

REQ X <INCLUDES> REQ Y

REQ Z <APPLIES_TO> REQ Y

The Selfstanding Set represented by REQ X will consist of REQ X, REQ Y and REQ Z.

The set of requirements that are explicitly included in a binding requirement are limited to “ICD” type of requirements. There could be confusion on how to interpret a binding as a Selfstanding Set from inclusion or not of other requirements (e.g. functional, non-functional). By convention:

- all other requirements that are not tagged as “ICD” and that do not have an <APPLIES_TO> relationship will be included in the Selfstanding Set.

- all other requirements that are not tagged as “ICD” and that do have an <APPLIES_TO> relationship will be included in the Selfstanding Set if there exist a path via relationship to a requirement that is part of the “ICD” or that is part of the ones identified in the line above.

C.2.6 “Testability" Attribute

Rationale

In the context of conformance/compliance it is necessary an attribute that indicates whether a specification is testable or not, and if so to what extent.

Possible values

Different standardisation bodies have their classification related to the testability of conformance (e.g. ISO, OASIS, W3C). In this case use of the ontology and nomenclature documented https://wiki.oasis-open.org/tab/TestingPolicy is proposed:

- <Conformance testable>
- <Interoperability testable>
- <Applicable but not testable>
- <Not applicable>
- <Unspecified>

<Unspecified> is an indication of a problem that needs to be solved.

Considerations

Each requirement is expected to have the same classification irrespective of Profile Part, Domain of Interest, Point of View or Role.

C.3 SWIM-TI specific requirement links

C.3.1 <ATMS Requirement> Linked Element Type

For this linked element type, programme guidelines only allow <SATISFIES> relationship. Additional relationship types are needed in the SWIM-TI context.

Table 84 provides the relationships applicable to the <ATMS Requirement> linked element type relationships for SWIM-TI specifications.

Solution specific REQ relationships	Description	Example	Link Type
Specialized specification <specializes> generic specification.	Requirement A specializes requirement B means that A inherits from B.	A: Synchronous R/R MEP. B: Synchronous R/R MEP implemented on top of SOAP/HTTP.	<SPECIALIZES><ATMS Requirement>
Low-level specification <satisfies> High-level specification.	Requirement A satisfies requirement B means that A covers high-level needs specified by B.	B: Message Encryption. A: XML Encryption.	<SATISFIES><ATMS Requirement>

Solution specific REQ relationships	Description	Example	Link Type
Constraining specification <applies to> specification	Requirement A provides constraints about requirement B.	B: XML Encryption. A: Encryption Key length.	<APPLIES_TO><ATMS Requirement>
Including specification <includes> specification.	Requirement A includes requirement B means that to cover A it is also needed to cover B.	A: SOAP 1.1 over HTTP 1.1 Interface "X". B: SOAP 1.1 shall be provided.	<INCLUDES><ATMS Requirement>

Table 84: SWIM-TI <ATMS Requirement> Linked Element Type relationships

For this linked element type, all the SWIM-TI REQ Trace tables are filled in as follows:

- Relationship: <SATISFIES> or <SPECIALIZES> or <APPLIES_TO> or <INCLUDES>
- Linked Element Type: <ATMS Requirement>
- Identifier: target requirement identifier.

Appendix D Subscription Management XML schema

This appendix provides the PJ.17-01 defined XML schema for subscription management messages described in §4.2.2.2.1.2.

Taking into account TRL6 validation activities, following changes have been implemented:

- Added additional faults (e.g. *DigitalSignatureValidationFault*).
- Added *ActiveSubscriptionsNotify* message.



SubscriptionManagementXSD.zip

Appendix E MS Excel export of PJ.17-01 requirements

This appendix provides MS Excel export of requirements included in this TS. Attached spreadsheet is automatically generated from the TS and it is provided just as supporting artefacts for requirements analysis. Furthermore, the spreadsheet is not maintained separately: it is a supporting artefact for a given TS edition.



PJ17-01 TRL6 TS Requirements

Appendix F SESAR and FAA Air-Ground SWIM comparison

This appendix provides a high level comparison between SESAR (Purple Profile) and FAA (Aircraft Access to SWIM - AAts) Air-Ground SWIM. The comparison is not expected to be exhaustive and complete: its purpose is to provide initial considerations that should be further assessed in a wide context from operational and technical perspectives.

The comparison is provided from different perspectives:

- Operational,
- Technical,
- Deployment.

Following references have been used:

- [59] Aircraft Access to SWIM (AAtS) Concept of Operations (ConOps), July 31, 2013.
- [60] Aircraft Access to SWIM Implementation Guidance Document, Version 2.0, 3/1/2013.
- [61] Aircraft Access to SWIM Full Data Exchange Technical Concept Paper, Version 1.0, 7/31/2013.

F.1 Operational perspective

From operational point of view both FAA and SESAR Air-Ground SWIM solutions address the same operational needs and scenarios.

The addressed ATM operational improvements depend on Air/Ground (A/G) information exchanges to enable a better situational awareness and collaborative decision making, with a focus on advisory information (supplemental information that is not necessary for and not directly interfering with the command and control of an aircraft).

In terms of operational scenarios, both solutions have been designed (for SESAR this is true at least for the SWIM infrastructure) adopting as reference the EUROCAE/RTCA ED-151/DO-308 (OSED for aeronautical information (AIS) and meteorological (MET) data link services).

Furthermore, for both current (i.e. limited to advisory information sharing) FAA and SESAR Air-Ground SWIM solutions, no safety impact are assumed. In particular, and adopting as reference the “what” identified in SESAR (refer to §4.2.2.1.3), the following safety objectives have been assumed:

- Ensure that any operational service(s) intended to be operated over the Air-Ground SWIM infrastructure have been evaluated by a reference authority as having no safety effect on civil air transport operations.
- Ensure that Air-Ground SWIM infrastructure integration to avionics system does not adversely impact existing aircraft type certificate(s), by targeting a minimal impact installation that is not increasing avionics systems complexity, so that any required Supplemental type certification (STC) only address minor changes.

F.2 Technical perspective

From technical point of view, a detailed comparison is not feasible mainly because the differences in the architectural framework adopted. SESAR Air-Ground SWIM design is more structured and complete: the design is described by applying architectural framework such as EATMA (which is in turn based on NAF 3.1) and ISO/IEC/IEEE 42010:2011 (refer to architectural viewpoints described in §4. Standard based architecture description is a must to have for a complete and unambiguous comparison.

However, a preliminary and high level comparison from technical perspective is provided in this section.

The layered view described in §4.2.1.1.3 and §4.2.1.2 could be considered applicable to both SESAR and FAA Air-Ground SWIM solutions, and in general to the SWIM concept. In particular the following layers have been identified in the SWIM context:

- SWIM enabled application layer (or SWIM service layer).
- SWIM infrastructure layer (or SWIM technical infrastructure layer).
- Network infrastructure layer (air-ground, ground-ground).

Taking into account the perimeter of this TS, the comparison is limited to the SWIM infrastructure layer. For what concerns the network infrastructure, both SESAR and FAA Air-Ground solutions are largely "network agnostic" relying on an IP based network with "*sufficient bandwidth to support the desired services*". SESAR Air-Ground SWIM provides more details such as Class of Services, multilink, and some performance figures. Further details are out of scope of this comparison but it is anticipated that word-wide IP based "connectivity" for SWIM enabled aircraft is required.

For what concerns the SWIM enabled application layer, two aspects are relevant:

- SWIM enabled service design and information models (WXXM, AIXM, etc.). This is an important aspect to be further assessed in order to harmonize SWIM services design and promoting operational and technical interoperability.
- Application-SWIM infrastructure interfacing layer that aims at allowing the SWIM enabled applications to consumed/provided SWIM services.

In the remaining part of this section the SWIM infrastructure layer and the application-SWIM infrastructure interfacing layer are further assessed.

In both solutions, the open standards based, reliable and secure SWIM technical infrastructure aims at enabling the integration of the aircraft into the SWIM network, thus giving it access to air/ground SWIM services (e.g. uplink and downlink of meteorological and aeronautical information). By adopting SESAR terminology, in both SESAR and FAA, the Air–Ground SWIM segment is a set of Aircraft and Ground functions that allow Aircraft SWIM Enabled applications to interact with Ground SWIM Enabled applications via provisioning and consumption of SWIM Services.

Overall, both solutions mainly provide messaging and security functions. In the context of SESAR Air-Ground SWIM infrastructure, these functions are described starting from the functional viewpoint (the "what") and then instantiating them in the technical viewpoint (the "how"). These functions are allocated to one or both of the "intermediaries" between SWIM service consumer and provider: Air SWIM Node and Ground SWIM Node. Furthermore, in SESAR a modular structure is applied by allocating requirements to mandatory or optional profile parts (refer to §A.3.4)

FAA Air-Ground SWIM infrastructure is also based on intermediary between SWIM service consumer and provider:

- (ground) National Airspace System (NAS) Enterprise Messaging Services (NEMS), that *include the messaging and management functions needed to support SWIM operations*.
- (ground) National Airspace System (NAS) Enterprise Security Gateway (NESG), that *is a framework for supporting mandated boundary protection services between SWIM and external entities. It provides a standardized scheme for connecting and managing connections to external users. It also enables a layered security scheme to provide defense in depth and provide a buffer between SWIM and external entities*.
- (ground) Data Management Service (DMS), that *is an intermediary service developed by entities not within the NAS and connects to SWIM through the NESG. The Data Management Service is that set of functions that are needed to manage connections between aircraft and the NESG. Additionally, it maintains a number of data sets needed to manage transactions with the Security Gateway, aircraft, and external users. Lastly it manages the communications links with the aircraft and SWIM as well as validating and filtering data and monitoring network performance*. In the overall architecture, there could be multiple DMSs. The DMS entity/intermediary is conceptually similar to Ground SWIM Node in SESAR Air-Ground SWIM infrastructure.
- (air) Aircraft Access to DMS, that *is a set of functions that manages the aircraft connection with the DMS in support of the intended use. These functions are hosted by a variety of onboard systems that may include, but not limited to, flight management, informational, video surveillance, and sensor systems*. It, conceptually, assimilates both SESAR Air SWIM Node and Aircraft SWIM enabled applications.

NEMS and NESG could be seen as FAA NAS specific "entities"/intermediaries required when consuming NAS services or when NAS SWIM enabled applications have to consume aircraft provided services. In the context of this comparison, what is considered really relevant are the DMS(s) and Aircraft Access to DMS. Indeed this also recognized by FAA in one of the identified challenge (Challenge #3): *interoperability of DMSs to multiple SWIMs (NAS, ANSPs and other enterprise data sources) infrastructures*.

The interoperability challenge at NESG – DMS and DMS - Aircraft Access to DMS interfacing layers could be mapped to SESAR Air-Ground SWIM architecture as follows:

- NESG – DMS: ground application – Purple Profile Ground SWIM Node.
- DMS - Aircraft Access to DMS: Purple Profile Ground SWIM Node – Air SWIM Node.

In both SESAR and FAA, the above challenge has been faced starting from "messaging patterns" identification and design.

In SESAR the technical use cases have been identified and described in §3.1.1.2. On top of other characteristics such as QoS, each technical use case is mainly characterized by MEP/cardinality (PS*-MEP, FDRR-MEP and FDRMR-MEP) and direction (uplink, downlink). Datalink modes from EUROCAE/RTCA ED-151/DO-308 have been then mapped to MEPs. The TS is driven by these technical use cases and the resulting interface bindings (ground application – Purple Profile Ground SWIM Node and Purple Profile Ground SWIM Node – Air SWIM Node interfacing layers) are all based on Purple Profile defined messaging capabilities over AMQP 1.0 core (one technology for all the technical use cases).

In FAA AAtS, following messaging patterns "types" have been identified for downlink and it is not clear if they may also apply to uplink:

- Messaging Pattern A: NAS Service Hosting a Web Service Operation

  This pattern requires each DMS to continuously push aircraft data to NAS Service and it is fully based on web service technology.

  In SESAR, all the interface bindings are AMQP 1.0 core based. A consumer (subscriber, publication message consumer) of aircraft provided data may subscribe and receive publication messages accordingly.

- Messaging Pattern B: DMS Hosting Request-Response Web Service

  This pattern requires each NAS Service to make a request to a DMS to consume aircraft data. In response, the DMS must provide a function that can connect and respond with aircraft data. All the message exchanges between a DMS and NAS Service will be fully based on the web service protocol.

  As anticipated above, in SESAR the web service protocol is not in the Purple Profile technologies catalogue. A consumer (requestor) of aircraft provided data may send a request message and receive one or more responses accordingly (FDRR-MEP and FDRMR-MEP respectively).

- Messaging Pattern C: DMS Hosting Pub-Sub Service using JMS

  Each DMS provides a service that publishes aircraft data into SWIM irrespective of whether a consumer is requesting it or not. This service enables the DMS to continuously push data into SWIM. If there is no active consumer, the data will be cleared out by an expiration timer (e.g., time-to-live).

  In SESAR the JMS protocol is not in the Purple Profile technologies catalogue and all the interface bindings are AMQP 1.0 core based. However, there are a number of (C)OTS and libraries claiming AMQP 1.0 core compliance and, on the other hand, providing JMS compliant API on top of AMQP (this mainly based on the draft OASIS mapping between JMS and AMQP).

- Messaging Pattern D: DMS Hosting Pub-Sub with Web Service Notification

  Each DMS provides a service that can notify consumers of available aircraft data. This service enables a DMS to send notification to its subscribed consumers of new/updated aircraft data by providing the web service parameters to consume the data. Subsequently, the NAS Service makes a request to the DMS to consume aircraft data based on the parameters contained within the notification. All the message exchanges between DMS and NAS service will be fully based on the web service protocol.

  In SESAR the web service / web service notification protocol is not in the Purple Profile technologies catalogue and all the interface bindings are AMQP 1.0 core based. A consumer (subscriber, publication message consumer) of aircraft provided data may subscribe and receive publication messages accordingly.

Taking into account the above, although the similar "messaging pattern" based approach has been adopted, unfortunately both "message patterns" and the technical interfaces are different in the two solutions resulting in a technical interoperability issue.

Further analysis should be then performed on messaging and security functions comparing SESAR Air-Ground SWIM infrastructure functional and technical viewpoints with capabilities allocated to DMS (refer to §3.2.1.1 in [60]) and Aircraft Access to DMS (refer to §3.2.1.2 in [60]).

In addition to messaging functions, the information security should be also further assessed and harmonized when impacting interoperability: *challenge #3* introduced above, and the related interfacing layers, concerns also security interoperability.

In SESAR, security functions have been identified as part of the security risk assessment. Functional and technical requirements have been then specified in the SESAR Air-Ground SWIM infrastructure functional and technical viewpoints (refer to §4.2.1.1.2, §4.2.2.3, §4.3.1.2 and §4.3.5). From security KPA perspective, design and validation activities carried out by SESAR Air-ground SWIM infrastructure concern more the "Implementation measures" focus area. "Impact Measures" is not faced because it does not concern technical validation activities and it cannot be carried out in isolation by this solution. "Effectiveness Measures" (e.g. "Supply-chain Security aspects addressed" PI) concerns more industrialization phase. Requirements could be specified but their validation is out of scope of technical validation activities.

Limiting this analysis only to the interfacing layers introduced above, the security functions specified in SESAR aim mainly at enabling protection of information transfer (authentication, authorization, authenticity, integrity, etc.) by composing point to point and end-to-end security mechanisms (refer to §4.2.2.3 and §4.3.5): TLS, HMAC, digital signature, etc.

In FAA AAtS, basic and few security needs/requirements have been also identified. The first main difference is the security need/requirement between DMS and NESG: *DMS Providers must utilize a VPN tunnel to connect to the NESG*. In SESAR, message and transport level security requirements have been identified without assuming any network level security mechanisms. Depending on the specific DMS, it could be not affordable to "support" different network level security mechanisms when connecting to different ANSPs and/or SWIM (e.g. EU, US).

Although not detailed, some requirements have been also provided about DMS - Aircraft Access to DMS security:

- Digital identity authentication,
- Digital identity based authorization,
- Use of cryptographic keys and mechanisms,
- Data confidentiality and integrity.

The above "requirements" are also addressed and detailed in SESAR by adopting the X.509v3 as digital identity. The level of detail available for FAA AAtS does not allow to provide a detailed comparison.

It could be assumed that harmonization effort will done in order to promote interoperability of security solutions addressing and properly composing message and transport level security. Furthermore, assuming that word wide X.509v3 will be adopted as digital identity, it remains also to address Identity provider(s)/CA(s) interoperability needs. Thera are a number of aspects concerning X.509v3 certificates profiles, CDPs, OCSP(s), etc. impacting interoperability: it could be not affordable if a DMS, that has to support/enable secure information sharing with multiple regions, is required to be able to handle (e.g.) different X.509v3 certificates profiles or extensions depending on the region.

Further considerations about CA/Identity management are addressed in the deployment perspective.

F.3 Deployment perspective

Taking into account the technical perspective analysis, the deployment options described in §4.2.3 are considered relevant when assessing FAA and EU SWIM deployment perspective.

When considering word wide deployment, the deployment options identified for the Ground Purple Profile in §4.2.3.2 become more and more relevant. Using FAA SWIM terminology, and assuming the analysis in §F.2 is accepted, the EU Ground SWIM Node deployment options could be considered also applicable to the DMS(s).

The reference and solution scenarios described in the TRL6 TVALR Appendix I High level Economic Appraisal [58] are valuable and concrete input to further analysis of word wide deployment options.

Same considerations apply to deployment options concerning Identity Management described in §4.2.3.4. The technical viewpoint in the SESAR Air-Ground SWIM infrastructure refers in general to CA irrespective of possible deployment. At technical level, the CA provides capabilities used by the Purple Profile enabled applications and SWIM Nodes irrespective of how the trust-relationship between subordinate CAs and/or root CAs is established.

In addition to regulations needs, word wide deployment options such as the Bridge CA and CA delegation (or hierarchical PKI) should be properly evaluated.

Appendix G PJ.17-01 requirements to be addressed in future activities

In this appendix, the requirements that are still in <in progress> status are reported. The reasons of such status are:

- the requirement was not successfully validated (refer to TVALR [58] requirements assessment), or
- the requirement was not covered by technical validation objectives because is more oriented to the target platform where the solution will be deployed, or
- the requirement was added following validation activities.

All these requirements are proposed to be addressed in future activities (e.g. industrialisation or deployment).

Identifier	Requirement	Category	Profile Part	In progress reason
REQ-17.01-TS-0110.0075	The SWIM-TI Audit shall allow to audit integrity and authenticity validation attempts according to the specific audit policy.	<Functional> <Security>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target platform where the SWIM node is deployed.
REQ-17.01-TS-0110.0250	The SWIM-TI Audit shall allow to audit authentication attempts according to the specific audit policy.	<Functional> <Security>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target platform where the SWIM node is deployed.
REQ-17.01-TS-0110.0251	The SWIM-TI Audit shall allow to audit authorization attempts according to the specific audit policy.	<Functional> <Security>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target

				platform where the SWIM node is deployed.
REQ-17.01-TS-0110.0095	The SWIM-TI Security shall record events with all additional data specified in the applicable service-specific Audit Policy.	<Functional><Security>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target platform where the SWIM node is deployed.
REQ-17.01-TS-0110.0260	The SWIM-TI Security shall provide tamper-proof storage of sensitive information by applying encryption and digital signature.	<Design><Functional><Security>	<PP Air Security+><PP Ground Security+>	Requirement not in scope of technical validation activities. This type of requirements is typically addressed and implemented as part of the overall security management solution in the target platform where the SWIM Node is deployed.
REQ-17.01-TS-0110.0265	The SWIM-TI Security shall allow to maintain sensitive information in an uncompromised condition for a configurable number of days to be defined either by policy or application level configuration.	<Design><Functional><Security>	<PP Air Security+><PP Ground Security+>	Requirement not in scope of technical validation activities. This type of requirements is typically addressed and implemented as part of the overall security management solution in the target platform where the SWIM Node is deployed.
REQ-17.01-TS-0110.0245	The SWIM-TI Security shall protect the overall SWIM-TI against overload resulting from: + Denial of Service Attack, or + Service Utilization above maximum levels.	<Functional><Security>	<PP Core>	Overload protection requirements could be linked to this requirement. However, overall this requirement has not be fully validated. It is out of scope of technical validation activities.
REQ-17.01-TS-0110.0105	The SWIM-TI Security shall allow to configure different monitoring strategies according to current security context.	<Functional><Security>	<PP Core>	Requirement partially covered by technical validation activities.

Company General Use

REQ-17.01-TS-0110.0100	The SWIM-TI Audit Policy shall at least include the following information: - The information which need to be recorded, - The user roles that must be provided with audit records, - The frequency of reporting or event type triggering the audit.	<Functional> <Security>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target platform where the SWIM node is deployed.
REQ-17.01-TS-0180.0095	The SWIM-TI shall provide mechanisms to statically define audit policies.	<Functional> <Interface>	<PP Core>	No complete policy based audit solutions have been developed and validated. This is typically an aspect to be further refined taking into account the overall security management solution adopted in the target platform where the SWIM node is deployed.
REQ-17.01-TS-0110.0255	The SWIM-TI Security shall include a functionality for reporting the handling of the following Security Incidents: + Denial of Service. + Intrusion. + Malicious or unauthorized software installation. + Reconnaissance (e.g. port scanning). + Physical damage. + Information compromise. + Software failure (with security implications).	<Functional> <HMI><Security>	<PP Air Security+><PP Ground Security+>	Requirement out of scope of technical validation activities.
REQ-17.01-TS-0380.0010	The SWIM Node availability shall be greater than or equal to the highest availability required for Purple Profile enabled SWIM services consumed/provided through it.	<Reliability>	<PP Core>	Requirement out of scope of technical validation activities. This requirement should be revised (e.g. adding availability measures) taking into account SWIM service level non-

				functional requirements.
REQ-17.01-TS-0380.0015	The availability of Air-Ground SWIM Nodes pair shall be greater than or equal to the highest availability required for Purple Profile enabled SWIM services consumed/provided through it.	<Reliability>	<PP Core>	Requirement out of scope of technical validation activities. This requirement should be revised (e.g. adding availability measures) taking into account SWIM service level non-functional requirements.
REQ-17.01-TS-0390.0020	The SWIM Node continuous unavailability shall be less than or equal to the lowest continuous unavailability required for Purple Profile enabled SWIM services consumed/provided through it.	<Reliability>	<PP Core>	Requirement out of scope of technical validation activities. This requirement should be revised taking into account SWIM service level non-functional requirements.
REQ-17.01-TS-0390.0025	The continuous unavailability of Air-Ground SWIM Nodes pair shall be less than or equal to the lowest continuous unavailability required for Purple Profile enabled SWIM services consumed/provided through it.	<Reliability>	<PP Core>	Requirement out of scope of technical validation activities. This requirement should be revised taking into account SWIM service level non-functional requirements.
REQ-17.01-TS-0400.0060	The retry mechanism shall allow to update the connection URIs parameter of the retry policy at run-time without restarting the software system/sub-system.	<Reliability>	<PP Ground Advanced><PP Air Advanced>	Currently only tested for application - SWIM Node connections. This should be also implemented for Air SWIM Node - Ground SWIM Node connections.
REQ-17.01-TS-0230.0015	End to end message latency for services of Category A shall be as follows: + Measurements: - 95% of the messages <= 20s - 98% of the messages <= 40s + Measurement conditions: - message size <= 2MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and	<Performance>	<PP Core>	Requirement not successfully validated by exercises. Provided figures have to be revised and validated during next phase taking into account service level requirements.

Company General Use

	link times excluded from the measurement). - Consolidated network bandwidth of 512Kbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.			
REQ-17.01-TS-0230.0020	End to end message latency for services of Category B shall be as follows: + Measurements: - 95% of the messages <= 30s - 98% of the messages <= 60s + Measurement conditions: - message size <= 2MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 512Kbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points:	<Performance>	<PP Core>	Requirement not successfully validated by exercises. Provided figures have to be revised and validated during next phase taking into account service level requirements.

Company General Use

	- Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.			
REQ-17.01-TS-0230.0025	End to end message latency for services of Category C shall be as follows: + Measurements: - 95% of the messages <= 100s - 98% of the messages <= 150s + Measurement conditions: - message size <= 20MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 2Mbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.	<Performance>	<PP Core>	Requirement not successfully validated by exercises. Provided figures have to be revised and validated during next phase taking into account service level requirements.
REQ-17.01-TS-0230.0030	End to end message latency for services of Category D shall be as follows: + Measurements:	<Performance>	<PP Core>	Requirement not successfully validated by exercises. Provided figures have to be revised and validated

Company General Use

	- 95% of the messages <= 150s - 98% of the messages <= 200s + Measurement conditions: - message size <= 20MBytes. - No “on the fly” compression. - Link, Session and Connection reuse (connection, session and link times excluded from the measurement). - Consolidated network bandwidth of 2Mbps, no congestions. - Transport and message level security in accordance with the interface bindings. - Normal load/no overload. + Observation points: - Times are measured at messaging resources level when the message is available for routing/distribution and when the message is ready for the consumption by the intended application level recipient.			during next phase taking into account service level requirements.
REQ-17.01-TS-0270.0225	Maintenance process shall be scheduled ensuring that CRLs are updated before they expire.	<Security>	<PP Core>	Requirement out of scope of technical validation activities.
REQ-17.01-TS-0270.0235	When the local CRL is not the current CRL or the CRL scope is not appropriate for the certificate in question, the peer shall either reject the certificate or accept a potentially revoked or compromised certificate depending on its Authentication policy.	<Security>	<PP Core>	Currently the validated solutions do not allow to accept a potentially revoked or compromised certificate.
REQ-17.01-TS-0270.0240	The CRLs update mechanisms shall be able to handled delta-CRL.	<Security>	<PP Ground Security+><PP Air Security+>	Although this is a capability provided out of the box by software products, this requirement has not been tested. This should be

				done in next phases (e.g. industrialization) taking into account also the evolution of SWIM Identity management capability configuration.
REQ-17.01-TS-0270.0245	The CRLs update mechanisms shall be able to handled CRL partitioning.	<Security>	<PP Ground Security+><PP Air Security+>	Although this is a capability provided out of the box by software products, this requirement has not been tested. This should be done in next phases (e.g. industrialization) taking into account also the evolution of SWIM Identity management capability configuration.
REQ-17.01-TS-0270.0300	OSCP response shall not exceed a defined maximum size.	<Security>	<PP Ground Security+><PP Air Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0305	OSCP providers shall be secure and authorized.	<Security>	<PP Ground Security+><PP Air Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0310	OCSP requestor shall be protected against OSCP replay attacks.	<Security>	<PP Ground Security+><PP Air Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0315	OCSP requestor shall be protected against OCSP Man-in-the-middle attacks.	<Security>	<PP Ground Security+><PP Air Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0320	Configuration files' integrity must be ensured.	<Security>	<PP Core>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0325	Alerts shall be emitted in case of unwanted configuration files modifications.	<Security>	<PP Air Security+><PP Ground Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0330	Configuration files integrity shall be monitored at maintenance time.	<Security>	<PP Air Security+><PP Ground Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0335	Administration accounts shall be personal.	<Security>	<PP Core>	New requirement added following the validation activities.

REQ-17.01-TS-0270.0065	Evidence of the correct execution of security functions shall be provided in the form of either an acknowledgement or auditing.	<Security>	<PP Air Security+><PP Ground Security+>	Requirement out of scope of technical validation activities.
REQ-17.01-TS-0270.0070	SWIM-TI audit logs shall be stored in a secure storage.	<Security>	<PP Air Security+><PP Ground Security+>	Requirement not in scope of technical validation activities. This type of requirements is typically addressed and implemented as part of the overall security management solution in the target platform where the SWIM Node is deployed.
REQ-17.01-TS-0270.0075	SWIM-TI audit data shall be stored in a storage location remote and independent from the system generating the audit data.	<Security>	<PP Air Security+><PP Ground Security+>	Requirement not in scope of technical validation activities. This type of requirements is typically addressed and implemented as part of the overall security management solution in the target platform where the SWIM Node is deployed.
REQ-17.01-TS-0270.0340	Security logs shall be audited.	<Security>	<PP Air Security+><PP Ground Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0345	Security auditing shall emit alerts.	<Security>	<PP Air Security+><PP Ground Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0350	Encryption keys length shall be at the state of art.	<Security>	<PP Core>	New requirement added following the validation activities.
REQ-17.01-TS-0270.0045	During or after power outage, security of running systems shall be protected.	<Security>	<PP Core>	Requirement out of scope of technical validation activities.
REQ-17.01-TS-0440.0130	IETF RFC 4033 Domain Name System Security Extensions (DNSSEC) shall be used for DNS based names resolution.	<Security>	<PP Air Security+><PP Ground Security+>	Although this is a capability provided out of the box by software products and it is transparent to SWIM Nodes/application when

Company General Use

				using logical names, this requirement has not been tested.
REQ-17.01-TS-0300.0015	Operational/SWIM enabled service(s) intended to be operated over the SWIM Purple profile for advisory information sharing shall have been evaluated by a reference authority as having no safety effect on air transport certificate holders' operations.	<Safety>	<PP Air>	Requirement out of scope of technical validation activities.
REQ-17.01-TS-0600.0123	In addition to basic operations, the Subscription handler shall be able to handle ActiveSubscriptionsNotify message.	<Interface>	<PP Air Advanced><PP Ground Advanced>	New requirement added following the validation activities.
REQ-17.01-TS-0600.0245	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to transfer information security using the AMQP footer, the following fallback solution should be provided: - Use the AMQP application properties section instead of the AMQP footer section, or both. - AMQP application properties containing same <key,value> pairs defined for AMQP footer. - Usage and further details concerning the fallback solution are documented. - When possible, to avoid to transfer over the Air/Ground connection the security information duplicated in AMQP application properties and footer sections.	<Interface><Security>	<PP Ground Security+><PP Air Security+>	New requirement added following the validation activities.
REQ-17.01-TS-0600.0250	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the	<Interface>	<PP Core>	New requirement added following the validation activities.

Company General Use

	user-id property, the following fallback solution should be provided: + Add the user-id information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “userid”. - value = string representation of the name-based UUID. + Usage and further details concerning the fallback solution are documented.			
REQ-17.01-TS-0600.0255	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the content-type property, the following fallback solution should be provided: + Add the content-type information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “contentType”. - value = string representation of the applicable IETF RFC 2046 MIME Media. + Usage and further details concerning the fallback solution are documented.	<Interface>	<PP Core>	New requirement added following the validation activities.
REQ-17.01-TS-0600.0260	In case, due to limitations of third-party software used to instantiate the Purple Profile, it is not possible to retain point-to-point and/or end-to-end the content-encoding property, the following fallback solution	<Interface>	<PP Core>	New requirement added following the validation activities.

Company General Use

	should be provided: + Add the content-encoding information also to the AMQP application properties section. + AMQP application property <key,value> pair defined as follows: - key = “contentEncoding”. - value = in accordance with REQ-17.01-TS-0600.0195. + Usage and further details concerning the fallback solution are documented.			
REQ-17.01-TS-0490.0015	The Communication Network Infrastructure shall provide IP routing.	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0020	The Communication Network Infrastructure shall allow to use Transmission Control Protocol (RFC 793).	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0030	The Communication Network infrastructure MTU max available shall be documented.	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0100	The Air/Ground Network Infrastructure should support IP fragmentation/reassembly of IPv4 data as specified in IETF RFC 791 to maximise bandwidth	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the

	usage.			responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0440.0120	The Communication Network infrastructure shall support IETF RFC 950, Internet Standard, Internet Standard Subnetting Procedure, August 1985 http://tools.ietf.org/html/rfc950.	<Interoperability>	<PP Ground><PP Air Advanced>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0010	The Communication Network Infrastructure should provide IPv4 (RFC 791) support.	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0005	The Communication Network Infrastructure shall provide IPv6 (RFC 8200) support.	<Interface>	<PP Ground><PP Air Advanced>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0440.0110	The Network infrastructure shall support IETF RFC 6434, Memo, IPv6 Node Requirements, December 2011 http://tools.ietf.org/html/rfc6434.	<Interoperability>	<PP Ground><PP Air Advanced>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0105	The Aircraft Information Network shall provide IPv6 (RFC 8200) support in accordance with AEEC 664 Part 3.	<Interface>	<PP Air Advanced>	Network requirement and, in addition, out of scope of technical validation activities.
REQ-17.01-TS-0490.0040	The Communication Network Infrastructure shall provide network traffic classification (Class of services) mechanisms	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used IPv6 and

Company General Use

	for handling QoS at network level.			CoSs from 14.2.4 FCI but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0045	The Air/Ground Network Infrastructure should provide at least two levels of CoSs: one level with guarantee of service (no congestion) and another with service best effort.	<Interface>	<PP Core>	Network requirement. The SWIM Node/application successfully used IPv6 and CoSs from 14.2.4 FCI but the responsibility of the requirement is demanded to solutions concerning the network layer.
REQ-17.01-TS-0490.0125	Application level messages integrity shall be ensured during all processing at Communications Network Infrastructure level.	<Security>< Design>	<PP Core>	Network requirement. The SWIM Node/application successfully used both IPv4 and IPv6 but the responsibility of the requirement is demanded to solutions concerning the network layer.

Table 85: In progress requirements

-END OF DOCUMENT-