



# Overview of current Air-Ground SWIM Security

Antonio Strano / Leonardo, [antonio.strano@leonardocompany.com](mailto:antonio.strano@leonardocompany.com)  
Pj17-01 Solution lead

PJ.17-01 Open Day, 5<sup>th</sup> July 2018  
*Leonardo Rome, Italy*



Founding Members



# Outline (30')



- SecRAM methodology & PJ.17-01 TRL4
- Overview of security controls concerning information in transmission
- Feedback from technical validation activities
- Q&A

# SecRAM methodology & PJ.17-01 TRL4 Methodology & DELs

- In the context of SESAR2020 Cybersecurity, PJ.17-01 has been identified as prioritized solution.
- Starting from TRL4, PJ.17-01 applied the SecRAM methodology involving in the security risk assessment other solutions (PJ.18-04).



# SecRAM methodology & PJ.17-01 TRL4

## Identified primary asset



| ID   | Type          | Within scope of security assessment | Outside Scope + Assumptions                                                                                                  |
|------|---------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| SC#1 | Inf. exchange |                                     | <b>Aircraft control data:</b><br>Assumption is that this data will not be transported nor affected by SWIM                   |
| SC#2 | Inf. exchange |                                     | <b>ATC Clearance, Instructions or Information:</b> Assumption is that this data will not be transported nor affected by SWIM |
| SC#3 | Inf. exchange | Advisory data                       |                                                                                                                              |
| SC#4 | Inf. exchange |                                     | <b>Airline business data:</b><br>Assumption is that this data will not be transported nor affected by SWIM                   |
| SC#5 | Inf. exchange |                                     | <b>Aircraft maintenance data:</b><br>Assumption is that this data will not be transported nor affected by SWIM               |
| SC#6 | Inf. exchange |                                     | <b>Passenger and entertainment data:</b> Assumption is that this data will not be transported nor affected by SWIM           |



| ID   | Primary Asset | Type        | Description                                   |
|------|---------------|-------------|-----------------------------------------------|
| PA#1 | Advisory data | Information | Aeronautical and meteorological advisory data |

# SecRAM methodology & PJ.17-01 TRL4 Security Assessment Report



- Supporting assets have been identified starting from end2end architecture (application, SWIM-TI and network layers).
- Impact assessment, risk evaluation and treatment have been provided according to the methodology, threats catalogue and identified assets (only SWIM-TI supporting assets).
- Detailed results are confidential and reported in the SAR Part IIB and Part IIC.

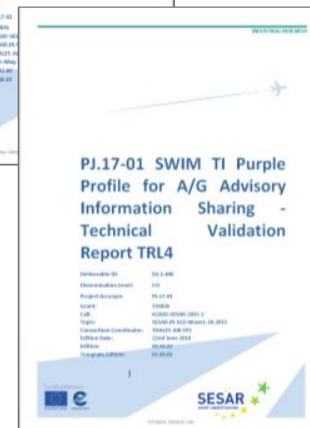
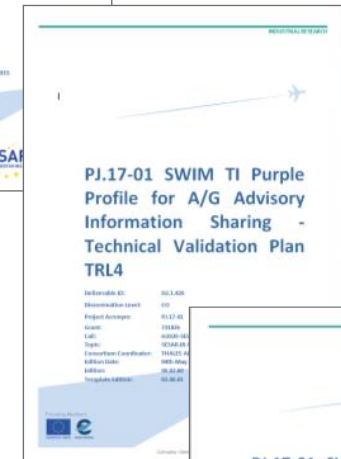
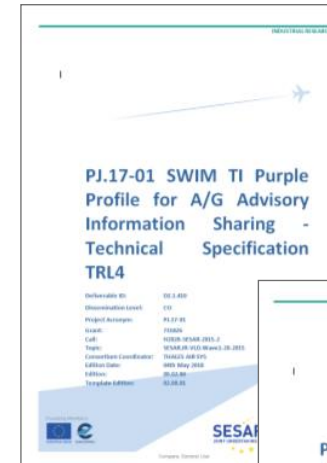


# SecRAM methodology & PJ.17-01 TRL4

## Security Controls

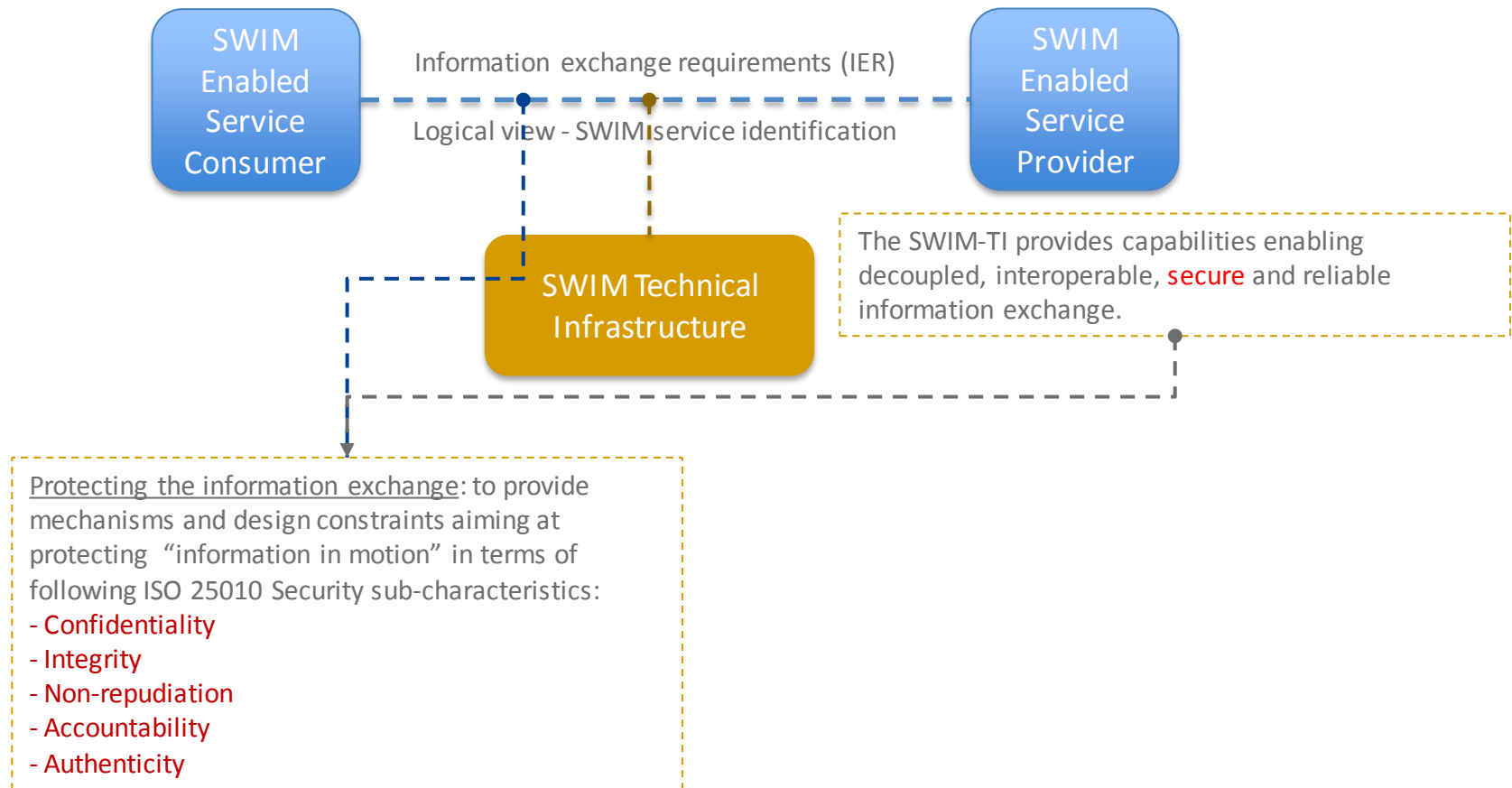


- Starting from MSSCs SoA additional (technical) security requirements have been provided in the TRL4 TS.
- Not all the identified security controls were considered subject of technical validation activities. For instance, security controls concerning procedures have been considered out of scope of technical validation activities.
- In the TVALP specific technical validation objectives concerning the security have been provided. In particular, only security controls related to “Security of information in motion” (Secure access controls - MSSC#6.1 and Information Transfer - MSSC#9.2) and logging and monitoring (MSSC#8.4) have been covered.
- Results from technical validation activities have been reported in the TVALR and they will be use during next maturity phase to improve both SAR and TS.



# Overview of security controls concerning information in transmission

## Needs



# Overview of security controls concerning information in transmission

## Technical architecture and end to end security

- Cryptographic algorithms and key sizes shall comply with NIST 800-131A recommendations.
- Taking into account the technical architecture (SWIM-TI layer intermediary nodes) it is needed to complement point to point (transport level) security mechanisms with end to end (message level) security mechanisms.
- Some end to end security needs are considered mandatory (e.g. message integrity and authenticity) and others (e.g. confidentiality) optional because depending on the specific SWIM service.

Table 1: Approval Status of Symmetric Algorithms Used for Encryption and Decryption

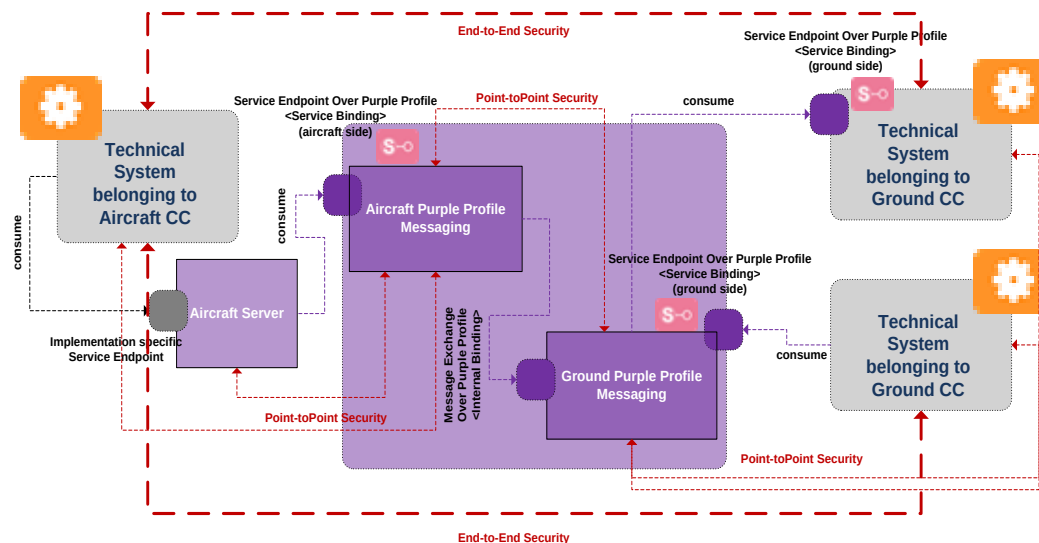
| Algorithm                                | Use                                              |
|------------------------------------------|--------------------------------------------------|
| Two-key TDEA Encryption                  | Restricted through 2015<br>Disallowed after 2015 |
| Two-key TDEA Decryption                  | Legacy-use                                       |
| Three-key TDEA Encryption and Decryption | Acceptable                                       |
| SKIPJACK Encryption                      | Disallowed                                       |
| SKIPJACK Decryption                      | Legacy-use                                       |
| AES-128 Encryption and Decryption        | Acceptable                                       |

Table 9: Approval Status of Hash Functions

| Hash Function                                                                  | Use                                           |                                                                                   |
|--------------------------------------------------------------------------------|-----------------------------------------------|-----------------------------------------------------------------------------------|
| SHA-1                                                                          | Digital signature generation                  | Disallowed, except where specifically allowed by NIST protocol-specific guidance. |
|                                                                                | Digital signature verification                | Legacy-use                                                                        |
|                                                                                | Non-digital signature applications            | Acceptable                                                                        |
| SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) | Acceptable for all hash function applications |                                                                                   |

Table 10: Approval Status of MAC Algorithms

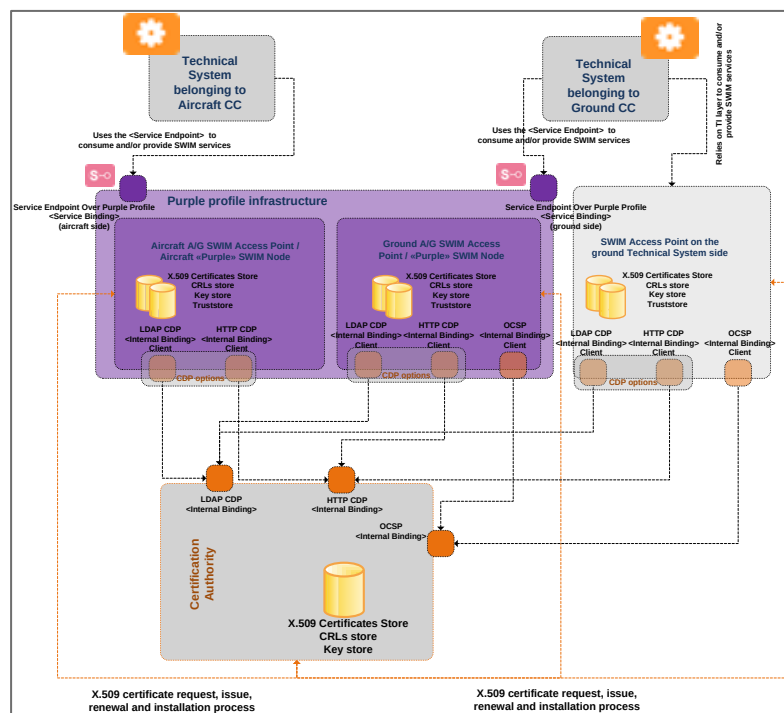
| (SHA-256, SHA-512) | MAC Algorithm     |                        | Use        |
|--------------------|-------------------|------------------------|------------|
|                    | HMAC Generation   | Key lengths < 112 bits | Disallowed |
|                    |                   | Key lengths ≥ 112 bits | Acceptable |
|                    | HMAC Verification | Key lengths < 112 bits | Legacy-use |
|                    |                   | Key lengths ≥ 112 bits | Acceptable |



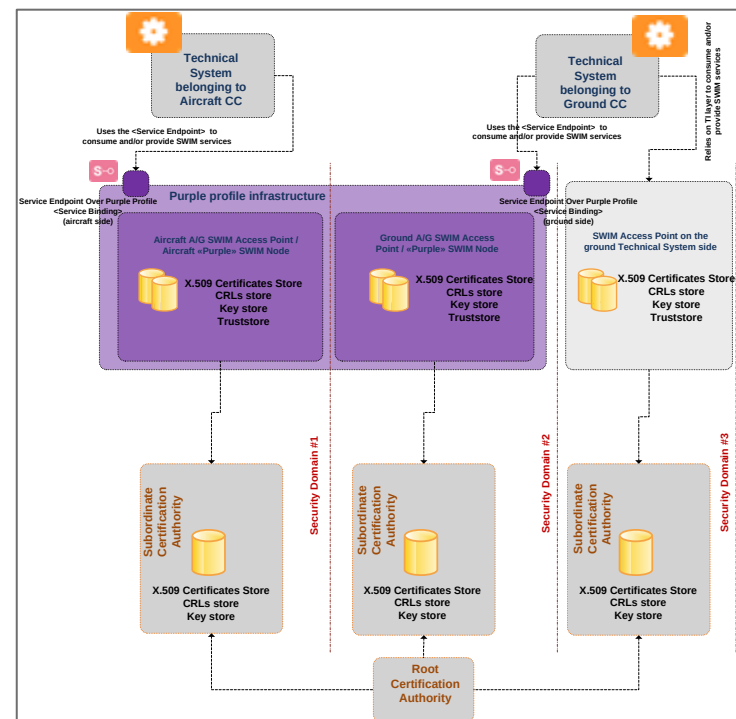
# Overview of security controls concerning information in transmission

## PKIs

- Most of (e.g. HMAC and symmetric encryption are also supported) the transport and message level security mechanisms are based on asymmetric cryptography.
- X.509v3 certificates and private keys are managed via PKI. As part of the technical validation activities protocols such as HTTP CDP and OCSP have been validated.



Reference technical architecture



One possible deployment option (additional ones could be based on Bridge CA, etc.)

# Feedback from technical validation activities

- Overall the validation activities successfully demonstrated the technical feasibility of most of the security controls concerning the "information in motion" specified in the TS.
- However, others security controls require further design, specification and validation effort. In particular requirements concerning security policies (definition & enforcement), logging and monitoring (reporting? SOC?), availability and fault tolerance have not been prototyped and/or validated.
- Furthermore, even if not subject to technical validation activities, overall SWIM security governance needs & related SCs have to be better formalized in collaboration with relevant ATM solutions (and also with PJ.14 – network layer).

| Validation Objective Identifier | Validation Objective definition                                                                                                                                                                                                                                                                                                                 | Solution Level Validation View          | EXE1 Coverage     | EXE2 Coverage     | EXE3 Coverage     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------|-------------------|-------------------|
| OBI-17.01-TRL4-TVALP-SECC.0001  | To validate the TRL4 maturity of the "Security of information in motion" security controls specified to protect confidentiality, integrity, authenticity and authorization security sub-characteristics of the information exchange according to the "Aircraft initiated Request/Response information exchange" use case (PPUC-01a).            | Partially validated by at least one EXE | Partially Covered | Partially Covered | Partially Covered |
| OBI-17.01-TRL4-TVALP-SECC.0002  | To validate the TRL4 maturity of the "Security of information in motion" security controls specified to protect confidentiality, integrity, authenticity and authorization security sub-characteristics of the information exchange according to the "Ground-based system provided Publish/Subscribe information exchange" use case (PPUC-02).  | Partially validated by at least one EXE | Partially Covered | Partially Covered | Partially Covered |
| OBI-17.01-TRL4-TVALP-SECC.0003  | To validate the TRL4 maturity of the "Security of information in motion" security controls specified to protect confidentiality, integrity, authenticity and authorization security sub-characteristics of the information exchange according to the "Ground-based system initiated Request/Response information exchange" use case (PPUC-03a). | Partially validated by at least one EXE | Partially Covered | Partially Covered | Partially Covered |
| OBI-17.01-TRL4-TVALP-SECC.0004  | To validate the TRL4 maturity of the "Security of information in motion" security controls specified to protect confidentiality, integrity, authenticity and authorization security sub-characteristics of the information exchange according to the "Aircraft provided Publish/Subscribe information exchange" use case (PPUC-04).             | Partially validated by at least one EXE | Partially Covered | Partially Covered | Partially Covered |
| OBI-17.01-TRL4-TVALP-SECC.0006  | To validate the TRL4 maturity of the "Security of information in motion" security controls specified to protect confidentiality, integrity, authenticity and authorization security sub-characteristics of the information exchange according to the "Aircraft initiated Request/Multi-Responses information exchange" use case (PPUC-01b).     | Partially validated by at least one EXE | Partially Covered | Not Covered       | Not Covered       |
| OBI-17.01-TRL4-TVALP-SECC.0007  | To validate the TRL4 maturity of the architecture and requirements concerning the X.509 certificates validation realized via one or more OCSP responders.                                                                                                                                                                                       | Validated by at least one EXE           | Fully Covered     | Not Covered       | Not Covered       |
| OBI-17.01-TRL4-TVALP-SECC.0009  | To validate the TRL4 maturity of the architecture and requirements concerning the CRLs updates realized via one or more HTTP CDPs.                                                                                                                                                                                                              | Validated by at least one EXE           | Fully Covered     | Not Covered       | Not Covered       |
| OBI-17.01-TRL4-TVALP-SECC.0011  | To validate the TRL4 maturity of the logging security controls.                                                                                                                                                                                                                                                                                 | Partially validated by at least one EXE | Partially Covered | Not Covered       | Partially Covered |
| OBI-17.01-TRL4-TVALP-SECC.0012  | To validate the TRL4 maturity of the monitoring security controls.                                                                                                                                                                                                                                                                              | Partially validated by at least one EXE | Partially Covered | Partially Covered | Not Covered       |





# Overview of current Air-Ground SWIM Security

---

## Thank you very much for your attention!



This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 730195



Founding Members



The opinions expressed herein reflect the author's view only.

Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.