



2019
World ATM Congress

SESAR walking tours



#PoweredBySESAR

Stand 849



Co-financed by the Connecting Europe
Facility of the European Union

SWIM Common PKI and policies & procedures for establishing a Trust framework

Speakers	
Florin STOIAN	Patrick MANA
ROMATSA	EUROCONTROL



2019 World ATM Congress





Co-financed by the Connecting Europe
Facility of the European Union

Expected Performance Benefits

- A common pan-European PKI (Public Key Infrastructure) and its associated framework that will ensure the interoperability of digital certificates within Europe and with other regions for all aviation stakeholders (ANSPs, Airports, Airspace users, Military, etc.)
- Improvement of the Security Key Performance Area thanks to the easier access to the digital certificates needed to secure the ATM communications
- Reducing PKI operations and corresponding costs at national and local level thus enabling the European ATM network to be run more cost-efficiently
- Improvement of the security of the exchange of information which should reduce the likelihood to get some disruption of services mainly due to corruption of information
- Facilitating and accelerating the provision and use of SWIM (System Wide Information Management) services by providing a solution that increases the security of the services



2019 World ATM Congress





Co-financed by the Connecting Europe
Facility of the European Union

Main information

Action title	<i>SESAR Deployment Programme Implementation - 2017</i>	Main AF	<i>AF5 - Initial System Wide Information Management</i>
Action number	<i>2017-EU-TM-0076-M</i>	Sub-AF	<i>S-AF 5.1 – Common infrastructure components</i>
Project Name	<i>SWIM Common PKI and policies & procedures for establishing a Trust framework</i>	Main family	<i>Family 5.1.4. - Common SWIM PKI and Cybersecurity</i>
Project Contributors	<i>30 Aviation Stakeholders (EUROCONTROL, 21 ANSPs, 3 Airports, 3 Airlines & 2 Military)</i>	Start / end date	<i>13 November 2018 - 31 December 2021</i>
Project Leader	<i>EUROCONTROL</i>	Planned costs	<i>10,018,306 €</i>



2019 World ATM Congress





Co-financed by the Connecting Europe
Facility of the European Union

Objectives

- Develop and deploy a common framework for both integrating local PKI deployments in an interoperable manner as well as providing interoperable digital certificates to the users of System Wide Information Management (SWIM)
 - Definition and development of a dedicated common PKI and its associated trust framework for Europe
 - Developing specifications for the systems needed to operate a PKI and its associated trust framework in order to produce and manage digital certificates
 - Integration and validation of the common PKI framework with some stakeholders to ensure the interoperability of digital certificates within Europe and with other regions
- Develop and deploy means in order to:
 - Secure the exchange of aviation related information
 - Provide identification and authentication of providers and consumers of aviation related information
 - Support the encryption when needed of aviation related information



2019 World ATM Congress



Description of work

1. Develop the Trust Framework policies and procedures
 - define the Policy Management Authority
 - develop / approve the initial Certificate Policy / Certification Practices Statement(s)
 - develop the Membership Agreement
 - develop interoperability/cross-certification framework & ensure interoperability with others PKIs
2. Develop Common PKI specifications (for both development and operations)
 - high-level architecture & functional technical specifications
3. Define the (SWIM) interfaces to the Common PKI
 - users interface & validation interfaces
4. Interface with SWIM Governance Project
5. Prepare the material for the potential launch of a CFT
6. Prepare all necessary material for operations
 - guidance for SWIM service providers & consumers



Co-financed by the Connecting Europe
Facility of the European Union

Key achievements

- Collect users needs:
 - SWIM services
 - many other users interested in benefiting from this solution (e.g. AMHS, future Data Link)
- Governance:
 - Relationships with SWIM Governance
 - Relationships with SES Digital Backbone initiative
- Interoperability with USA (FAA):
 - Plan to conduct interop tests
 - Definition of interop scenarios
- Consistency/link with global initiatives:
 - Initial contribution to ICAO/INNOVA project supported by ANC/13



2019 World ATM Congress





Co-financed by the Connecting Europe
Facility of the European Union

**Thank you very much
for your attention!**



2019 World ATM Congress





2019
World ATM Congress

SESAR walking tours



#PoweredBySESAR

Stand 849

GNSS Threats (Interferences)

SUPPORTED BY
SESAR
JOINT UNDERTAKING

gmv
INNOVATING SOLUTIONS

in Boella
ISMB
Istituto Superiore Mario Boella

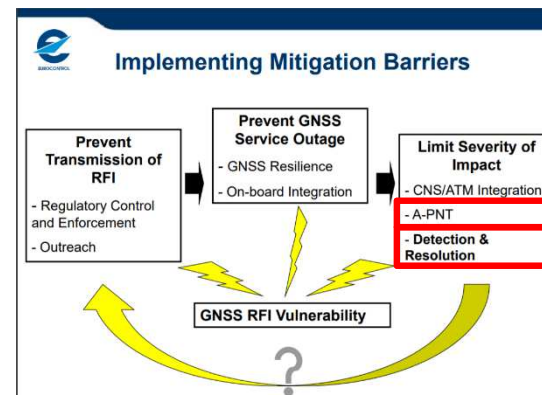
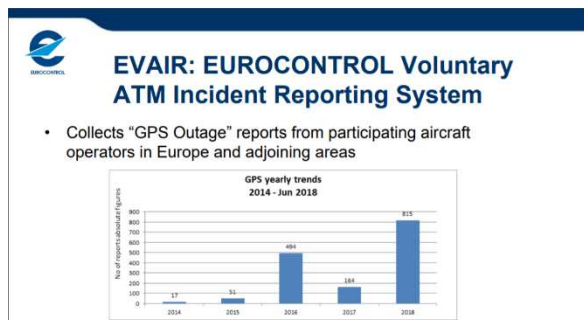


- **Context (GNSS interferences in aviation)**

GNSS RFI Mitigation: International Efforts to Protect Aviation

David Duchet & Gerhard BERZ / EUROCONTROL NAV & CNS Unit

58th Civil GPS Service Interface Committee Meeting / Miami, 24 September 2018



2019 World ATM Congress



GATEMAN: Objectives



- **Mitigation Barrier (MB1)**

Novel concept for GNSS interferences management.

Detection and localization of jamming on-board the aircraft.

Detection and localization of spoofing on-board the aircraft.

Detection and localization based on existing aircraft equipment (minimizing cost of retrofit and forward-fit).

Multi-Constellation/Multi-Frequency (i.e. GPS L1/Gal E1 and GPS L5/Gal E5a).

- **Mitigation Barrier (MB2)**

Application of 5G ground cell stations networks as A-PNT (Alternative Position, Navigation and Timing) technology.

- **Mitigation Barrier (MB3)**

Application of “spoofing monitoring” to mitigate the effects of spoofing.



2019 World ATM Congress



GATEMAN: Assumptions



- **Interference source**

Source on-ground (2D localization).

Static or quasi-static source (negligible speed compared to the aircraft).

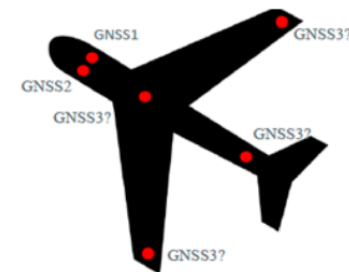
1 single source.

- **Aircraft (minimize retrofit)**

Omnidirectional GNSS antennas.

GNSS antennas on top of the fuselage (used for navigation).

3 GNSS antennas (existing aircrafts are equipped with 2).



2019 World ATM Congress



GATEMAN: Benefits



- **Deactivation of jamming and spoofing**

GATEMAN enables fast localization of the source.

ANSP and the National RF Spectrum Agency will receive accurate localization of the source to deactivate it, reducing the duration of the impact.

- **Traffic rerouting**

GATEMAN provides the localization of the source and the estimation of the affected volume.

ATC mitigates the operational impact of interference thanks to rerouting traffic to areas not affected by the interference.



2019 World ATM Congress



Funding



Call id	H2020-SESAR-2016-2
Topic	SESAR-ER3-05-2016 Enabling Aviation Infrastructure: CNS Scope. <i>Projects are expected to propose ideas for combining existing on-board and ground equipment for enhancing CNS capabilities. Solution for integrated CNS solutions and the implications of having one technology performing the three services at the same time can be studied (single point of failure..).</i>
Funding scheme	RIA (Research and Innovation Actions)
Grant Agreement No.	783183
Project	GATEMAN
Start date	01/01/2018
End date	31/12/2019



Further information:

<http://gateman.gmv.com/>

Project Coordinator:

Alberto de la Fuente
afuente@gmv.es



2019 World ATM Congress





2019
World ATM Congress

SESAR walking tours



#PoweredBySESAR



Co-financed by the Connecting Europe
Facility of the European Union

Stand 849



Co-financed by the Connecting Europe
Facility of the European Union



Creating local security operation center

Ref. No 2016_062_AF5,
Project Leader – BULATSA

SPECIFIC GRANT AGREEMENT No
INEA/CEF/TRAN/M2016/1351536



2019 World ATM Congress



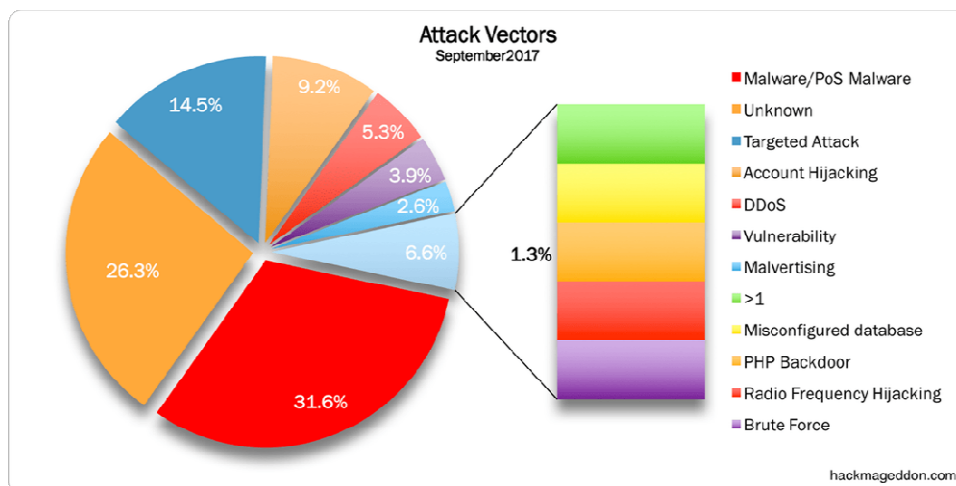
Creating Local Security Operation Center

“There are two types of companies: those who have been hacked and those who don’t yet know they have been hacked.”

John Chambers
Former CEO of Cisco Systems

So, a security breach is not a IF but a WHEN (and how badly).

Discovering and preventing of increasingly complex and sophisticated security attacks is the main reason organizations develop a Security Operations Centers



The average length of time that cyberattacks go undetected is a worrying 146 days, while some Advanced Persistent Threat activities can remain undetected for years.

Creating Local Security Operation Center



- The objective of the Implementation Project is to build a platform (hardware, software, people, procedures), providing reliable cyber defense of IT infrastructure of BULATSA against conventional and modern advanced cyber threats.
- The implemented solution represents a platform for monitoring, analysis and control of logs, network traffic, system files and incident management. It has been consolidating and managing the network and critical systems cyber-security events/incidents in a centralized capability;
- The platform is able to collect and share cyber-security events/incidents between the Security Operation Center of BULATSA, the national CERT and any other stakeholders from the ATM community.



2019 World ATM Congress



Event sources and collection methods

An analyst needs three things in order to perform competent network monitoring:

1. An initial tip-off capability such as a signature- or behavior-based IDS/antivirus. This includes the ability to leverage custom signatures and full details on the signature or behavior that fired.

2. NetFlow records that show a summary of communications to and from the hosts listed in tip-off information, days or weeks before and after the tip-off fired.

3. The packet capture for the packet(s) that triggered the alert, preferably for the full session (PCAP).


Threat Intelligence

- External threat intelligence
- Internal threat intelligence
- Indicators of compromise


Network Activity
/Security

- Firewall
- IDS/IPS
- Vulnerability scanner
- Malware sandbox
- Web proxy
- NetFlow


Endpoint Activity
/Security

- Endpoint (AV/IPS/FW)
- ETDR
- OS logs
- DHCP
- DNS
- Patch mgmt.


Authorization
Users/Roles

- Active Directory
- LDAP
- CMDB

- Operating System
- Database
- VPN, AAA, SSO



2019 World ATM Congress



29 JUN
2018

BULATSA INAUGURED A SECURITY OPERATIONS CENTER



BULATSA inaugurated its own Security Operations Center (SOC).

The project for its construction is implemented through co-financing from the Cohesion Fund of the European Commission under Connecting Europe Facility.

The project is one of its kind amongst the projects currently being implemented with funding from the European Commission and entirely follows the latest trends in the field of cyber-threat protection.

Examples of triggered alerts



- TOP 20 WEB requested IPs;
- Brute Force Login Attempts;
- TOR Outbound Attempts;
- AD – created accounts;
- AD – changed passwords;
- Cleartext Passwords by Service;
- Suspicious files;
- AD – deleted accounts;
- Privilege escalation for users and processes;
- AD – disabled accounts;
- Generating events for nonexistent users in AD;
- Suspicious Web activity;
- Locked user accounts;
- AD – changed user account;
- Communication with risky IPs;
- IPv4 Vertical Port Scans;





Co-financed by the Connecting Europe
Facility of the European Union



Thank you!

Daniela Vasilieva



2019 World ATM Congress





2019
World ATM Congress



SESAR
walking
tours



#PoweredBySESAR

Stand 849

Securing SESAR Solutions

- While the benefits of the SESAR solutions are well recognised, digitalisation, automation and interconnectivity open up new vulnerabilities which call for specific cybersecurity measures
- Some contributions from Leonardo for the Security of SESAR Solutions are listed below:
 - SESAR 1 heritage: WP16 Security Risk Management Methodology
 - SESAR PJ17.01 - SWIM Purple Profile Security:
 - Transport Level security, implementing TLS with PKI infrastructure
 - End to End Message Security (application layer) over several transport links
 - TRL4 validated in 2018; TRL6 to be validated in 2019
 - SESAR PJ14.02.06 - AEROMACS: implementation of Security specifications
 - SESAR PJ14.02.01 – LDACS
 - Definition of Secure Architecture Requirements
 - Security Risk Assessment
 - SESAR PJ16.03 - Virtual centre study , including Cybersecurity
- Beyond SESAR: Pioneering ATM Security in the FP7 funded GAMMA Project
 - The goal of GAMMA – Global ATM Security Management – was to develop solutions to the emerging ATM vulnerabilities backed up by practical proposals for their implementation



2019 World ATM Congress

Company Internal



Delivering Cybersecurity for the SESAR ATM Ecosystem

- To win the security war it is necessary to first recognize that Security represents an evolving, ever-changing and persistent challenge to ATM
- Delivering ATM Security should be seen as an evolving and continuous process completely integrated in the ATM system lifecycle.
- ATM Security should ensure that the systems are also prepared for the after-effects of an attack as well as preventing it in the first place.



2019 World ATM Congress

Company Internal



Securing the Operation of SESAR systems

Secure by Design

Secure by Configuration

Secure by Operation

- Protecting the SESAR ecosystem applying Secure by Lifecycle approach
- From 'Secure by Design' to 'Secure by Operation'
- Cutting edge technologies at the service of the SESAR Ecosystem



2019 World ATM Congress

Company Internal



Blockchain Enforced Integrated Access Control

The diagram is divided into two main sections: **SmartTAG TECHNOLOGY** and **BLOCKCHAIN TECHNOLOGY**.

SmartTAG TECHNOLOGY illustrates a system where physical tags (represented by small orange squares) are linked to a **Network**. The network connects to **Reader** devices, which in turn connect to an **NFC Middleware** (depicted with a snake icon). This middleware is linked to a **HYPERLOGGER** (depicted with a stack of disks). Below this, a hand holds a physical tag, and a **Student Case Solutions** scenario is shown with icons for **Manufacturing**, **Transportation**, **Distribution center**, and **Retail**. A central banner reads **NFC Smart in Smart World Applications**. An **Access Control** section shows people walking through a gate.

BLOCKCHAIN TECHNOLOGY illustrates a decentralized ledger system. It shows **Transactions (authenticated)** being processed through a series of **Nodes** (represented by orange squares) and **Validators** (represented by blue circles). The process involves **Validating Contents** and **Consensus**. The final output is a **REGISTRO (DECENTRALIZZATO E IMMUTABILE) ACCESSI - PRESENZE - USCITE** (Decentralized and Immutable Register of Accesses - Presences - Exits).

Registration in a private/consortium level blockchain of the detected presence or absence of the personnel



User access to ATC application

2019 World ATM Congress

Company Internal



Immutable recordings of lifecycle events through Blockchain



Cutting edge technologies at the service of the SESAR Ecosystem

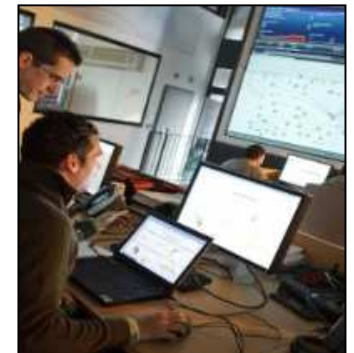
Protecting the SESAR ATM Environment:

Decision Support System (DSS) in support of ATM continuity and cyber resilience

- DSS uses Artificial Intelligence algorithms and a Big Data Analytics & IoT engine to determine the necessary protection and action steps to be taken in order to neutralise cyber attacks on ATM systems
- The system supports organisations to decide on the proper remediation actions to be taken to ensure business continuity and to minimise the consequences of dangerous and damaging cyber incidents.

Cyber Threat Assistance (CTA)

- CTA simplifies the management of cyber threats exploiting Artificial Intelligence for the implementation of the innovative 'Curiosity Learning' concept, allowing the autonomous completion of the cyber knowledge base, which represents the central repository in which all security information is stored. Curiosity Learning opens the way for interacting with the knowledge base through questions and answers using natural language.



2019 World ATM Congress

Company Internal



Securing SESAR Solutions



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 699238



2019 World ATM Congress

Company Internal





2019
World ATM Congress

SESAR walking tours



#PoweredBySESAR

Stand 849

GNSS Threats (Interferences)

SUPPORTED BY
SESAR
JOINT UNDERTAKING

gmv
INNOVATING SOLUTIONS

in Boella
ISMB
Istituto Superiore Mario Boella

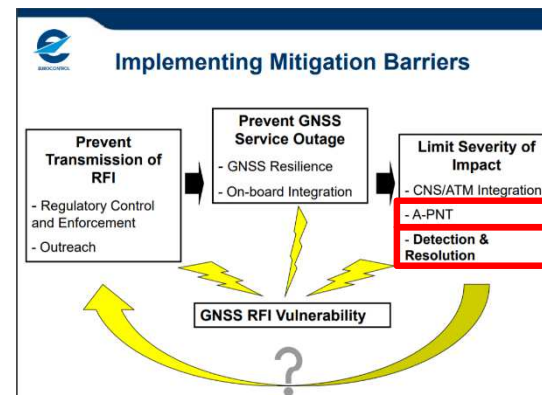
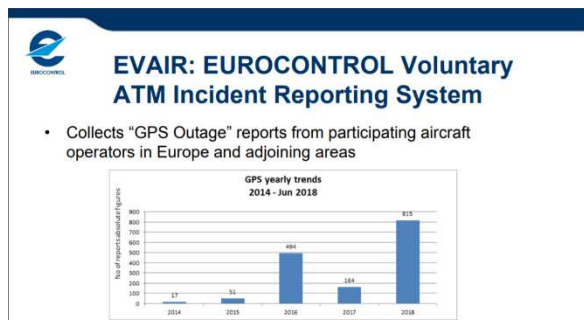


- **Context (GNSS interferences in aviation)**

GNSS RFI Mitigation: International Efforts to Protect Aviation

David Duchet & Gerhard BERZ / EUROCONTROL NAV & CNS Unit

58th Civil GPS Service Interface Committee Meeting / Miami, 24 September 2018



2019 World ATM Congress



GATEMAN: Objectives



- **Mitigation Barrier (MB1)**

Novel concept for GNSS interferences management.

Detection and localization of jamming on-board the aircraft.

Detection and localization of spoofing on-board the aircraft.

Detection and localization based on existing aircraft equipment (minimizing cost of retrofit and forward-fit).

Multi-Constellation/Multi-Frequency (i.e. GPS L1/Gal E1 and GPS L5/Gal E5a).

- **Mitigation Barrier (MB2)**

Application of 5G ground cell stations networks as A-PNT (Alternative Position, Navigation and Timing) technology.

- **Mitigation Barrier (MB3)**

Application of “spoofing monitoring” to mitigate the effects of spoofing.



2019 World ATM Congress



GATEMAN: Assumptions



- **Interference source**

Source on-ground (2D localization).

Static or quasi-static source (negligible speed compared to the aircraft).

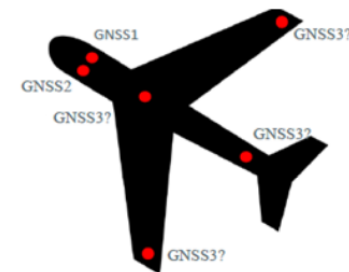
1 single source.

- **Aircraft (minimize retrofit)**

Omnidirectional GNSS antennas.

GNSS antennas on top of the fuselage (used for navigation).

3 GNSS antennas (existing aircrafts are equipped with 2).



2019 World ATM Congress



GATEMAN: Benefits



- **Deactivation of jamming and spoofing**

GATEMAN enables fast localization of the source.

ANSP and the National RF Spectrum Agency will receive accurate localization of the source to deactivate it, reducing the duration of the impact.

- **Traffic rerouting**

GATEMAN provides the localization of the source and the estimation of the affected volume.

ATC mitigates the operational impact of interference thanks to rerouting traffic to areas not affected by the interference.



2019 World ATM Congress



Funding



Call id	H2020-SESAR-2016-2
Topic	SESAR-ER3-05-2016 Enabling Aviation Infrastructure: CNS Scope. <i>Projects are expected to propose ideas for combining existing on-board and ground equipment for enhancing CNS capabilities. Solution for integrated CNS solutions and the implications of having one technology performing the three services at the same time can be studied (single point of failure..).</i>
Funding scheme	RIA (Research and Innovation Actions)
Grant Agreement No.	783183
Project	GATEMAN
Start date	01/01/2018
End date	31/12/2019



Further information:

<http://gateman.gmv.com/>

Project Coordinator:

Alberto de la Fuente
afuente@gmv.es



2019 World ATM Congress

