2019 World ATM Congress

SESAR walking tours

#PoweredBySESAR  Stand 849
SWIM Common PKI and policies & procedures for establishing a Trust framework

<table>
<thead>
<tr>
<th>Speakers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Florin STOIAN</td>
<td>Patrick MANA</td>
</tr>
<tr>
<td>ROMATSA</td>
<td>EUROCONTROL</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Action title</th>
<th>SESAR Deployment Programme Implementation - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action number</td>
<td>2017-EU-TM-0076-M</td>
</tr>
<tr>
<td>Project Name</td>
<td>SWIM Common PKI and policies &amp; procedures for establishing a Trust framework</td>
</tr>
<tr>
<td>Project Contributors</td>
<td>30 Aviation Stakeholders (EUROCONTROL, 21 ANSPs, 3 Airports, 3 Airlines &amp; 2 Military)</td>
</tr>
<tr>
<td>Project Leader</td>
<td>EUROCONTROL</td>
</tr>
<tr>
<td>Main AF</td>
<td>AF5 - Initial System Wide Information Management</td>
</tr>
<tr>
<td>Sub-AF</td>
<td>S-AF 5.1 – Common infrastructure components</td>
</tr>
<tr>
<td>Main family</td>
<td>Family 5.1.4. - Common SWIM PKI and Cybersecurity</td>
</tr>
<tr>
<td>Start / end date</td>
<td>13 November 2018 - 31 December 2021</td>
</tr>
<tr>
<td>Planned costs</td>
<td>10,018,306 €</td>
</tr>
</tbody>
</table>
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
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
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
Thank you very much for your attention!
GNSS Threats (Interferences)

- **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
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)**
  

• **Mitigation Barrier (MB3)**
  
  Application of “spoofing monitoring” to mitigate the effects of spoofing.
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).
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.
## Funding

<table>
<thead>
<tr>
<th>Call id</th>
<th>H2020-SESAR-2016-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>SESAR-ER3-05-2016</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Enabling Aviation Infrastructure: CNS</td>
</tr>
<tr>
<td></td>
<td>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..).</td>
</tr>
<tr>
<td>Funding scheme</td>
<td>RIA (Research and Innovation Actions)</td>
</tr>
<tr>
<td>Grant Agreement No.</td>
<td>783183</td>
</tr>
<tr>
<td>Project</td>
<td>GATEMAN</td>
</tr>
<tr>
<td><strong>Start date</strong></td>
<td>01/01/2018</td>
</tr>
<tr>
<td><strong>End date</strong></td>
<td>31/12/2019</td>
</tr>
</tbody>
</table>
Creating local security operation center

Ref. No 2016_062_AF5,
Project Leader – BULATSA

SPECIFIC GRANT AGREEMENT No
INEA/CEF/TRAN/M2016/1351536
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.
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.
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).
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;
Thank you!

Daniela Vasilieva
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.
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.
Securing the Operation of SESAR systems

- 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
Cutting edge technologies at the service of the SESAR Ecosystem

Blockchain Enforced Integrated Access Control

Protecting ATC applications through event correlation enforced by secure and immutable blockchain technology
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
2019 World ATM Congress

SESAIR walking tours

#PoweredBySESAIR

Stand 849
GNSS Threats (Interferences)

- **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
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)**

- **Mitigation Barrier (MB3)**
  Application of “spoofing monitoring” to mitigate the effects of spoofing.
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).
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.
## Funding

<table>
<thead>
<tr>
<th>Call id</th>
<th>H2020-SESAR-2016-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>SESAR-ER3-05-2016</td>
</tr>
<tr>
<td></td>
<td>Enabling Aviation Infrastructure: CNS</td>
</tr>
<tr>
<td><strong>Scope.</strong></td>
<td>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..).</td>
</tr>
<tr>
<td>Funding scheme</td>
<td>RIA (Research and Innovation Actions)</td>
</tr>
<tr>
<td>Grant Agreement No.</td>
<td>783183</td>
</tr>
<tr>
<td>Project</td>
<td>GATEMAN</td>
</tr>
<tr>
<td><strong>Start date</strong></td>
<td>01/01/2018</td>
</tr>
<tr>
<td><strong>End date</strong></td>
<td>31/12/2019</td>
</tr>
</tbody>
</table>


Project Coordinator: Alberto de la Fuente afuente@gmv.es