Importance of IATF to FAA

Rob Segers NAS ISS Architect

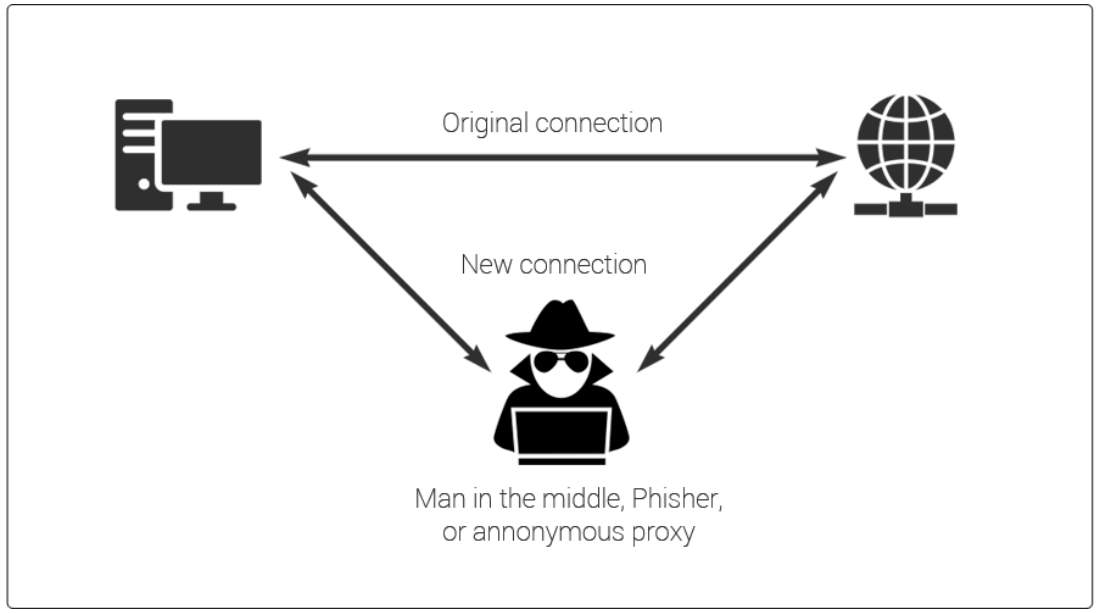
June 2021

Problem Statement

- The cost of fit for purpose networks and the use of protected spectrum limits the ability to grow the network connectivity, bandwidth and worldwide ATM automation integration required to grow aviation capacity and the integration of Unmanned Aircraft Systems
- The use of ubiquitous network peering across commercial networks including unprotected spectrum will require end to end information integrity between information producer and consumer to assure network trust and safety

Man in the Middle (MITM) Attacks: an Aviation Threat

- Man-in-the-middle(MITM) attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation
- The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected party
- A MITM attack allows the attacker to eavesdrop on the conversation between the parties, or to actively intervene in the conversation to achieve some illegitimate end

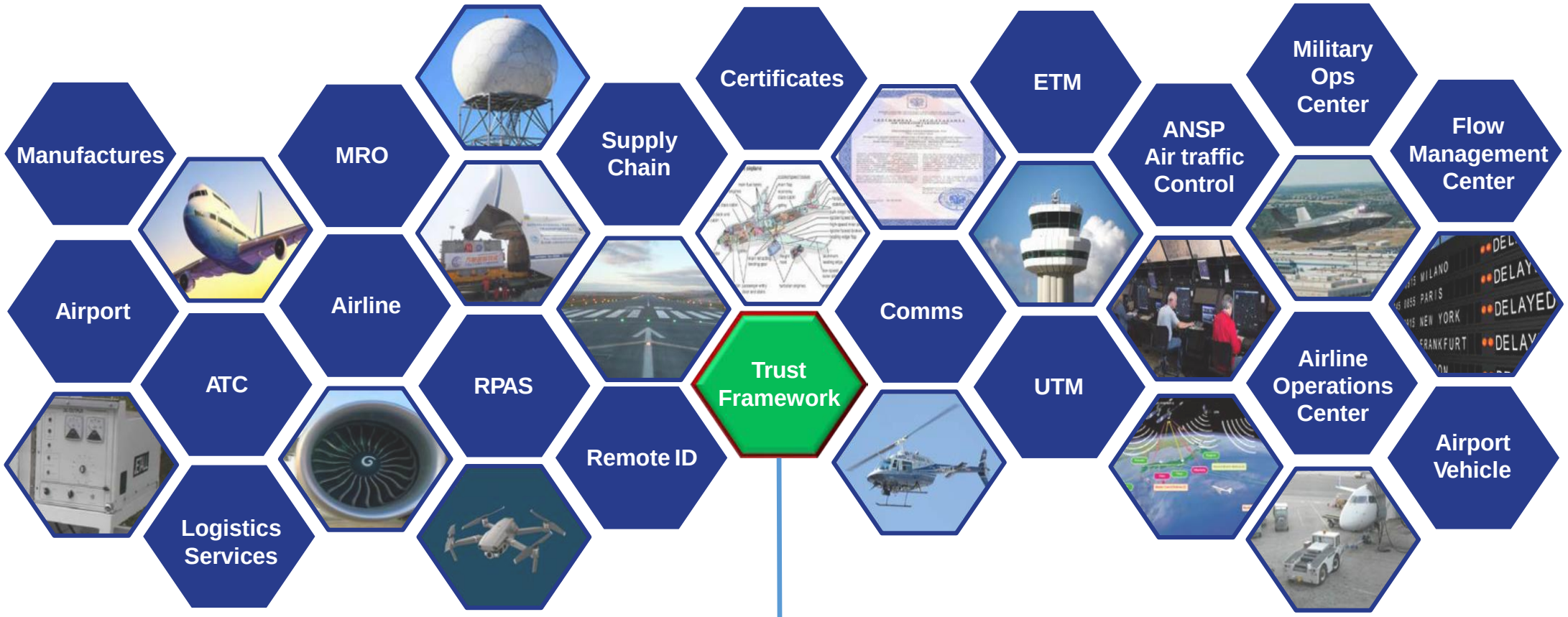


- A MITM attack can also occur by modifying information at rest (e.g. stored on a cloud server)

Problem Statement (continued)

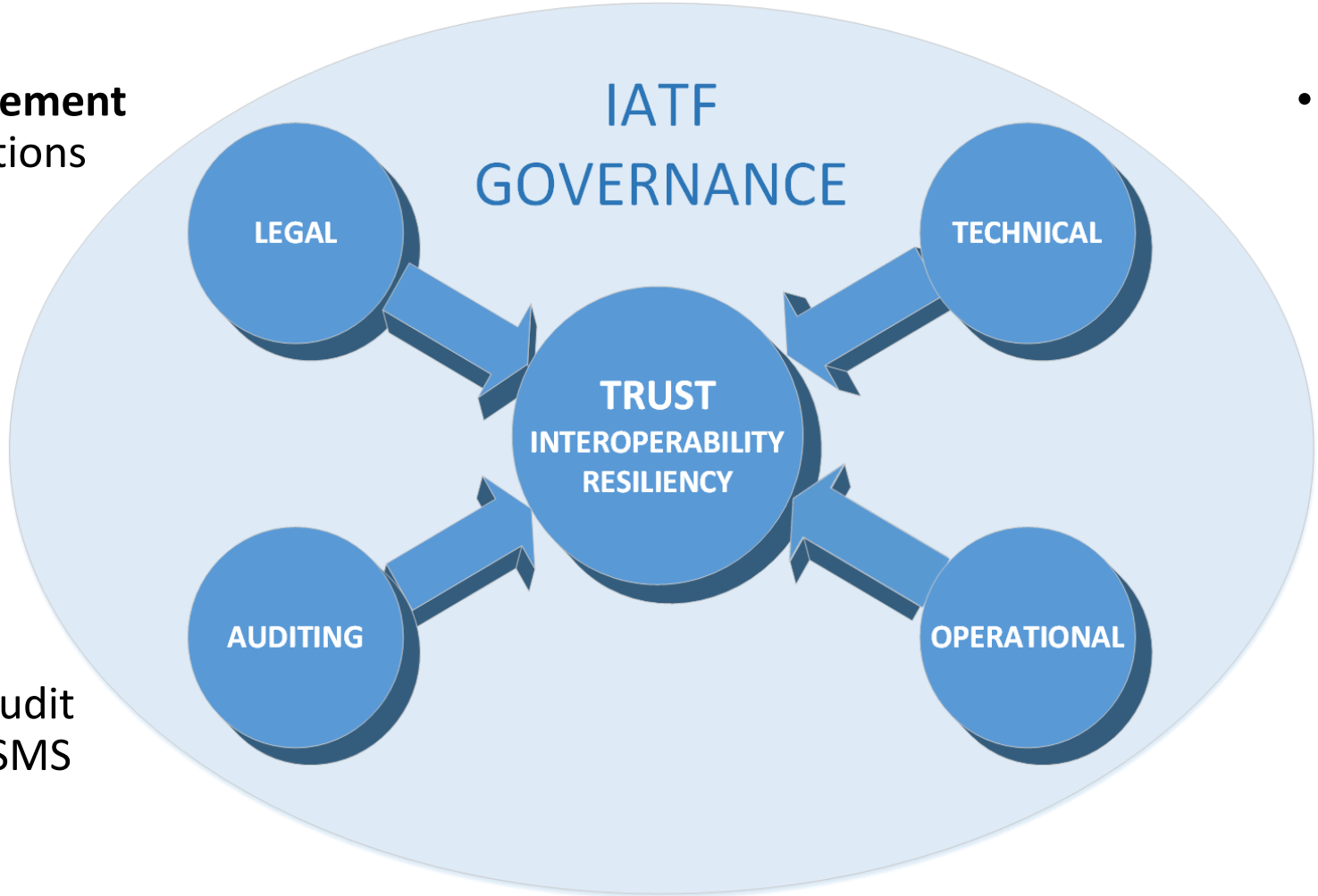
- Current compliance to standards and regulations does not provide identity and information security interoperability
- As a result of the lack of information security interoperability, there is no guarantee of end to end information protection
- Regulatory oversight (e.g. Hierarchical compliance verification) through ICAO auditing regulators and regulators auditing service providers does not provide security interoperability
- Information security interoperability (Trust) is currently established organization by organization and on a project by project basis
  - not scalable
  - complex
  - costly
  - increase of attack surface
  - lack of harmonization undermines confidence in information protection

Common Need Across the Ecosystem… Establish Trust and Resiliency



Operationalization of the Trust Framework
International Aviation Trust Framework (IATF)

- **Unified legal agreement**
  - Terms and conditions
  - Liabilities
  - Indemnifications
  - Warranties



- **Managed performance based requirements**
  - Trusted Identities
    - Identity policy
  - Trusted Networks
    - Network policy

- **Industry based audit practice**
  - e.g. Web trust Audit
  - e.g. ISO 27001 ISMS

- **Managed services**
  - Trust Anchor
  - Domain Naming
  - Network addressing
  - Security Monitoring
  - Interoperability Lab

Importance of IATF to FAA

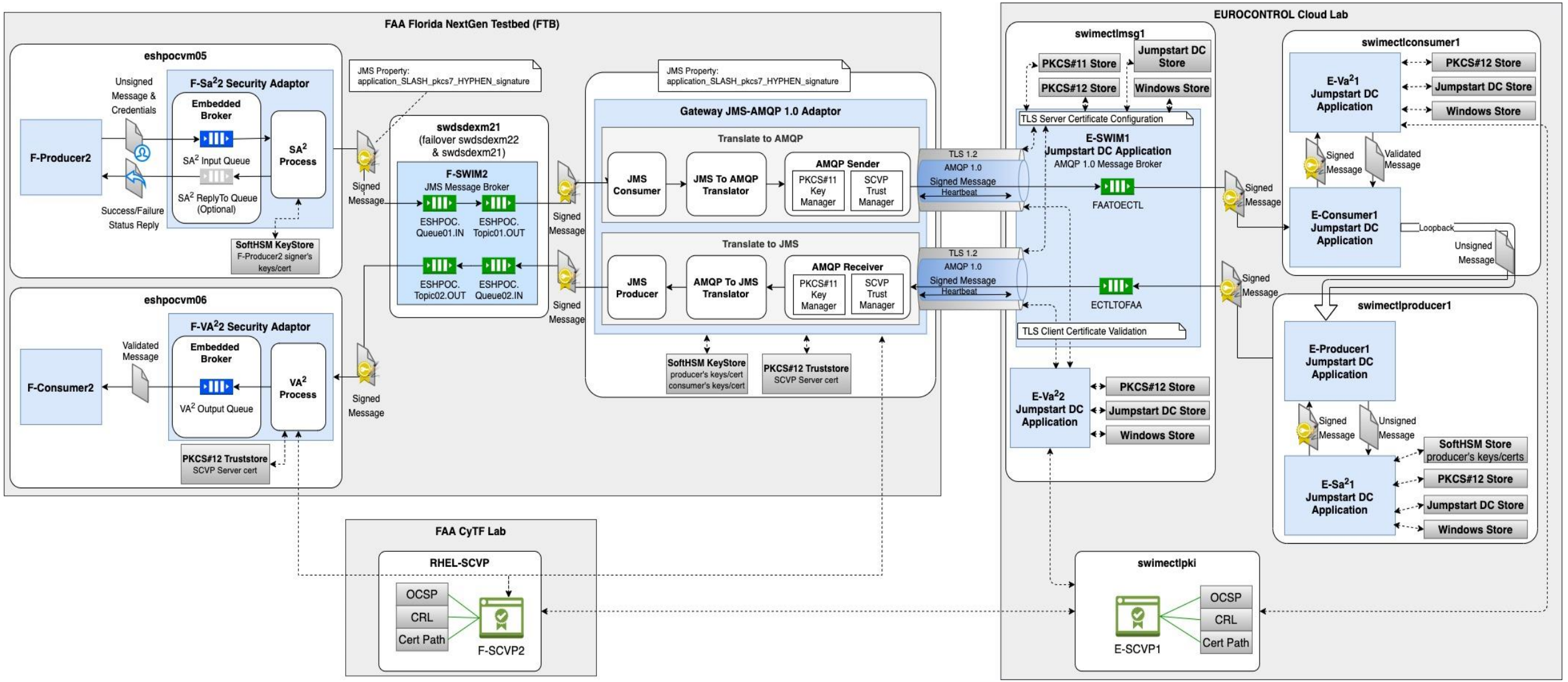
- North American Interactions between FAA and Nav Canada for Canadian international flights.
- North American Interactions between FAA within Services a la Navegacion en el Espacio Aereo Mexicano(SENEAM) in Mexico.
- Transition to IP networks and SWIM.
- Need for Federated Identity and Access Rights to secure internal FAA and international transactions

Enterprise Security Harmonization Proof Of Concept

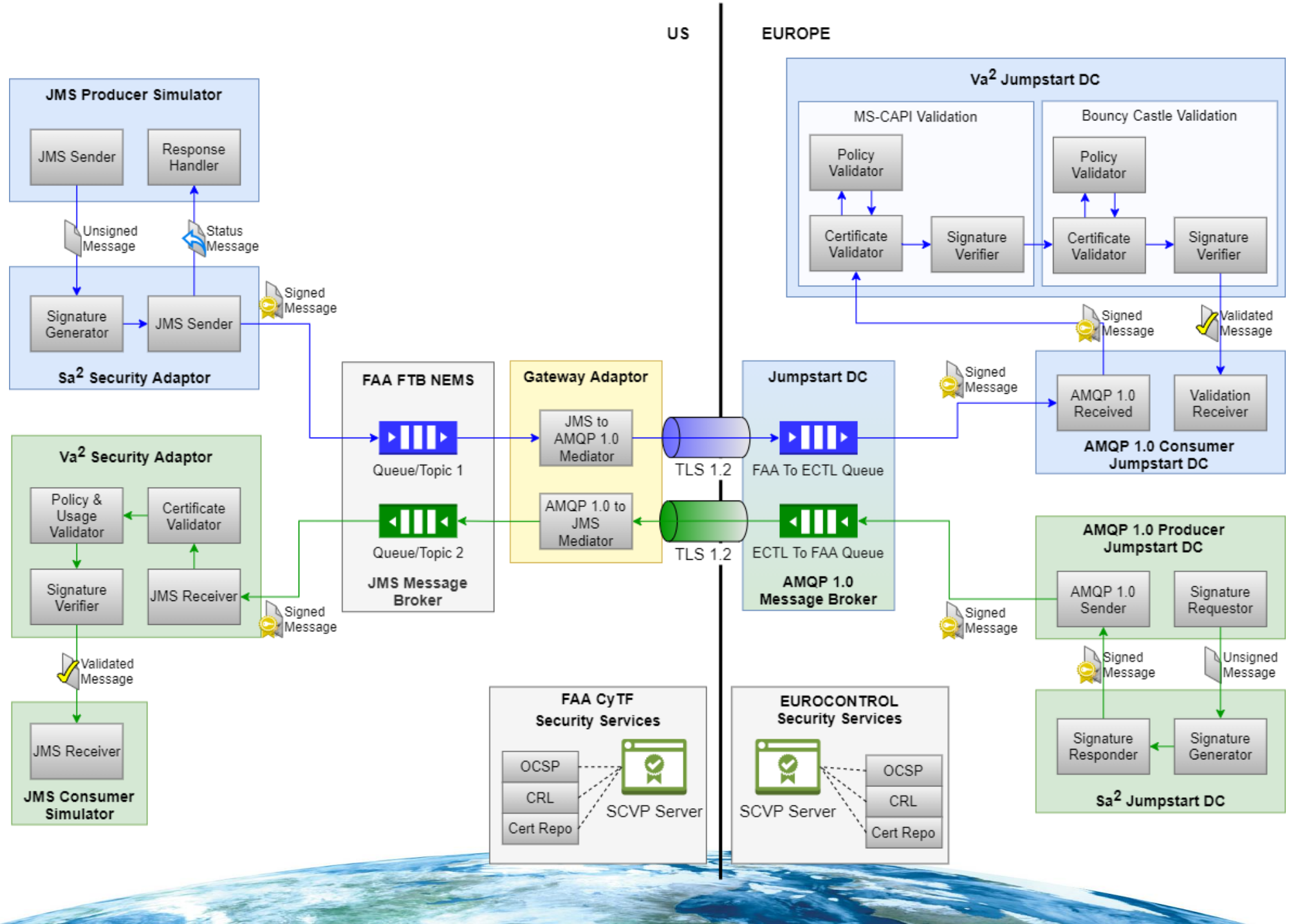
Testing the IATF Identity management approach

- The Enterprise Security Harmonization Proof Of Concept (ESHPOC) was started as part of the Coordination Plan (CP) 1.8 Enterprise Security between FAA NextGen and EU SESAR with as goal to
  - ➢Harmonize enterprise security between NextGen and SESAR
  - ➢Establish a proof of concept of the Trust Framework Study Group (TFSG) identity management approach between Europe and the US
  - ➢Show security interoperability between Europe and the US SWIM leveraging multiple Public key Infrastructure (PKI) methods to establish trust
- The TFSG has harmonized the International Aviation Trust Framework (IATF) PKI Certificate Policy (CP) used for ESHPOC

Detailed ESHPOC System Architecture



Simplified System Architecture



ESHPOC Main achievements - Security Interoperability

- ✓ **Integrity protected SWIM** messages can now be mediated between Java Message Service [FAA] and Advanced Message Queuing Protocol (AMQP) 1.0 [EU] implementations

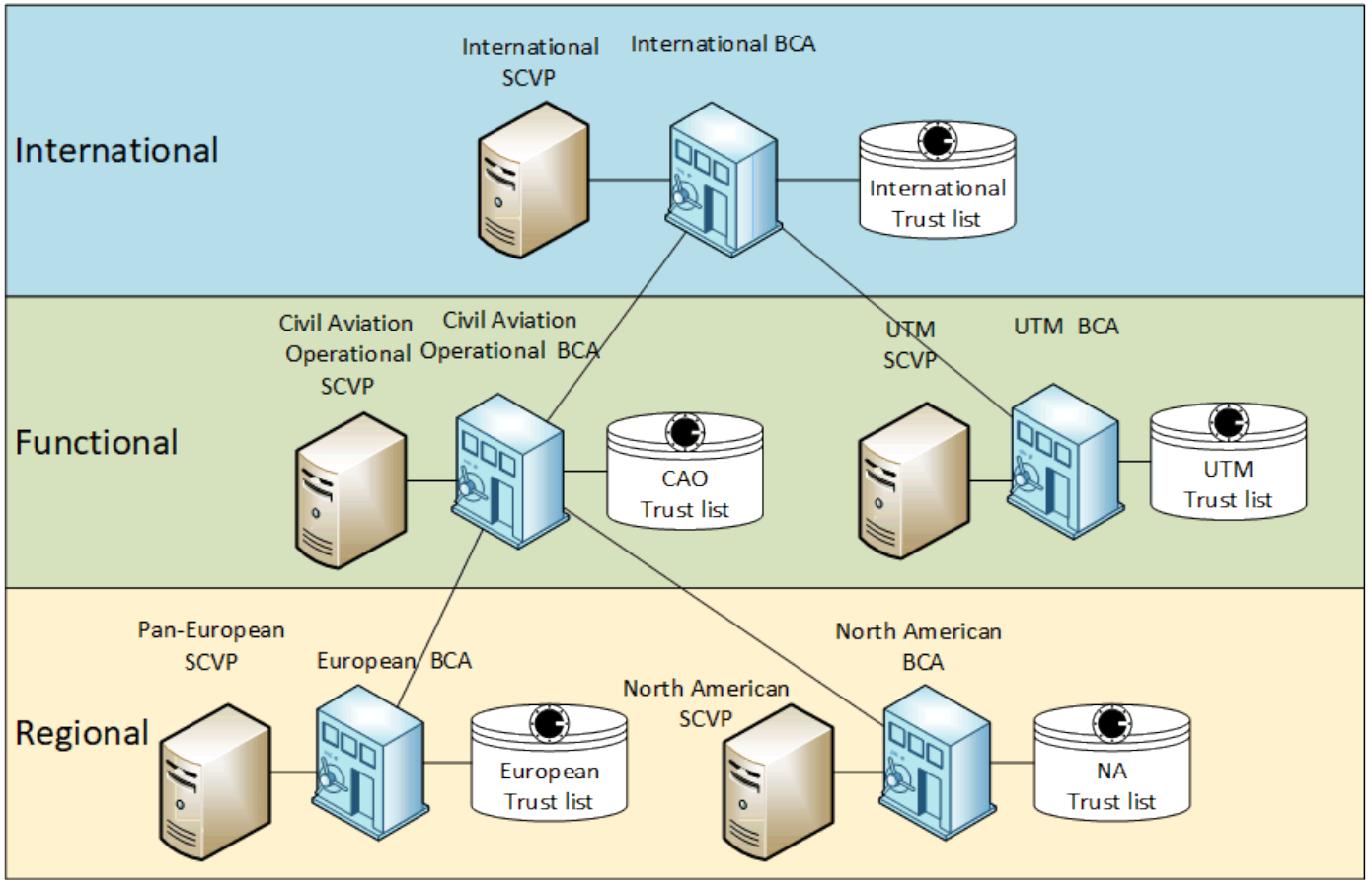
- ✓ **Signing as a Service** (Sa2) and **Validation as a Service** (Va2) in the context of SWIM message exchange between international organizations is now feasible

- ✓ **Sa2 and Va2 are backwards compatible** and allow organizations to implement independently

- ✓ **Validation of fit** for purpose SWIM Public Key Infrastructure (PKI) certificates using SWIM specific policies is now feasible

ESHPOC Main achievements (continued)

Trust between international CA's through the use of a **Bridge Certificate Authority** (BCA) and **Certificate Trust List** (CTL) can be established and should be used at the international, functional and regional level.



Hierarchy allows scaling and scope management

ESHPOC Gap analysis - Findings

- To ensure **interoperability**, the use of CTL requires the development and adoption of a standardized CTL schema that is fit for aviation purposes.
- SCVP COTS vendors should implement **blacklisting and validation of certificates** with multiple policies
- Some COTS certificate validation products are **not compliant with RFC 5055 SCVP** and have limitations
- Certificate validation boundary cases demonstrate potential **trade-offs between safety and security**

ESHPOC Gap analysis - Recommendations

- Develop a **Specification for mediation** between AMQP 1.0 and JMS
- **Cryptographic Message Syntax (CMS)** used to handle end to end message level security CMS has proven its efficiency and robustness and a standard CMS profile should be adopted
- The study of and **standardization of international federated tokens** is recommended as a follow-up project in particular to address scalability issues raised by Multiple Certificate Policy identifiers

Future FAA needs for IATF Alignment

- Operate an enterprise wide PKI using a certificate policy that meets the IATF requirements.
- Manage Digital Identities using an enterprise wide Policy Management Authority (PMA).
- Expand the use of federated identities to federate access for external users.
- Incorporate GRAIN requirements into SWIM and all external interfaces.
- Active participation in the operationalization and membership of the IATF

Questions?