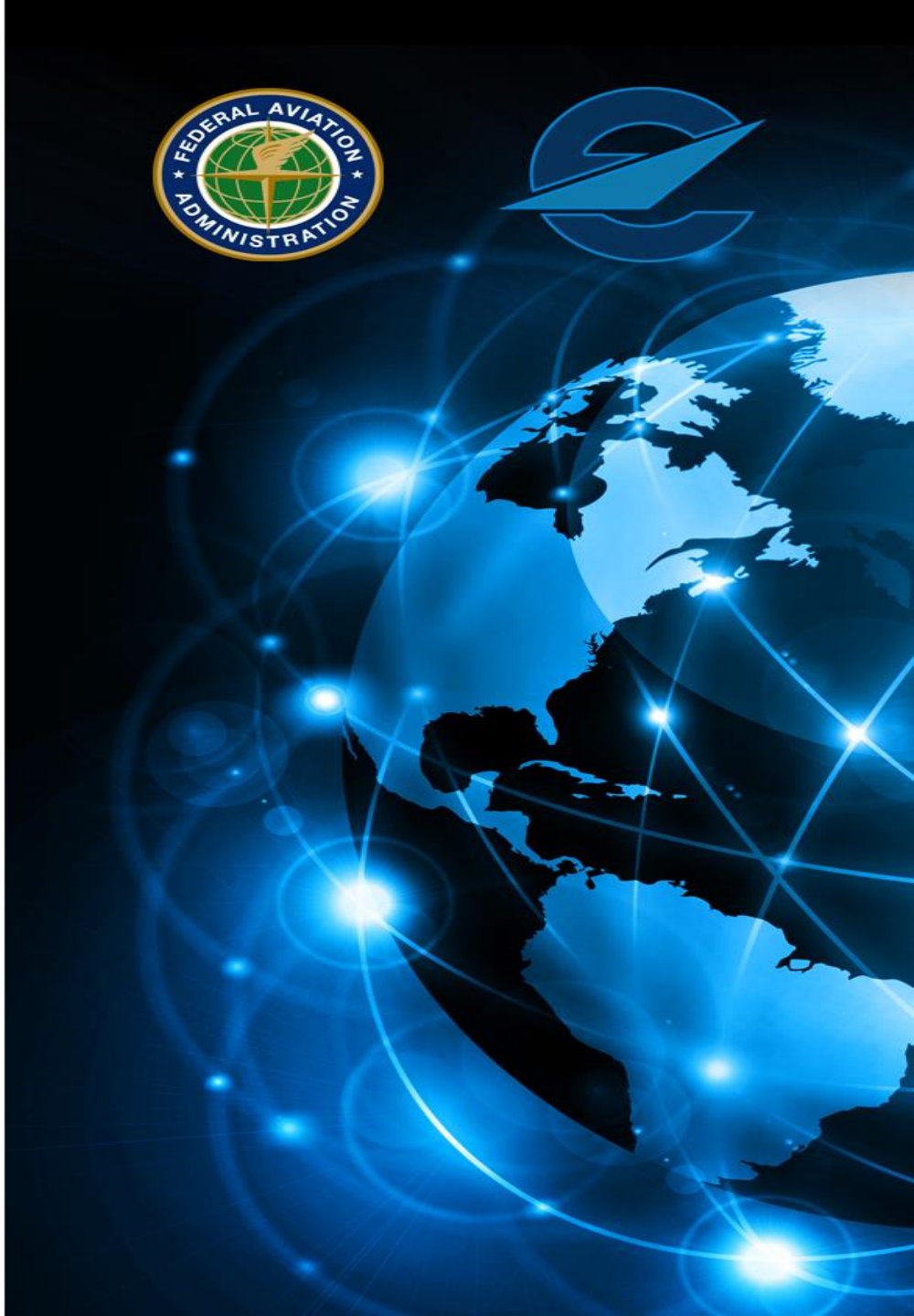
Enabling GRAIN

Securing against Man in the Middle attacks



Presented to: ATIEC 2019

By: Rob Segers,

NextGen ISS Architect

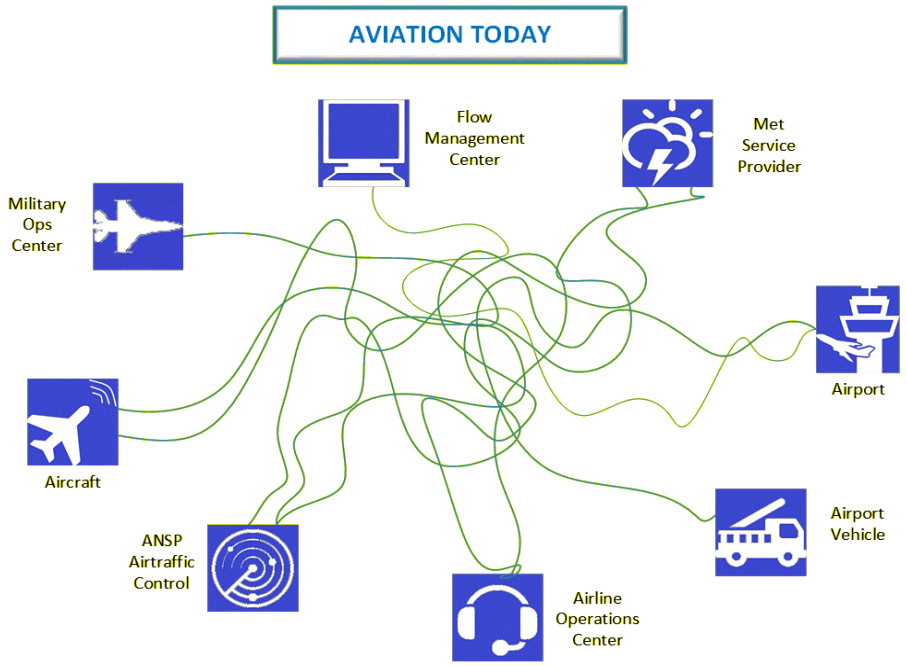
Date:

Aviation Information World – Forecasting the Future

Enabling Global Resilient Aviation Information Network (GRAIN)

- **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 Areal 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**

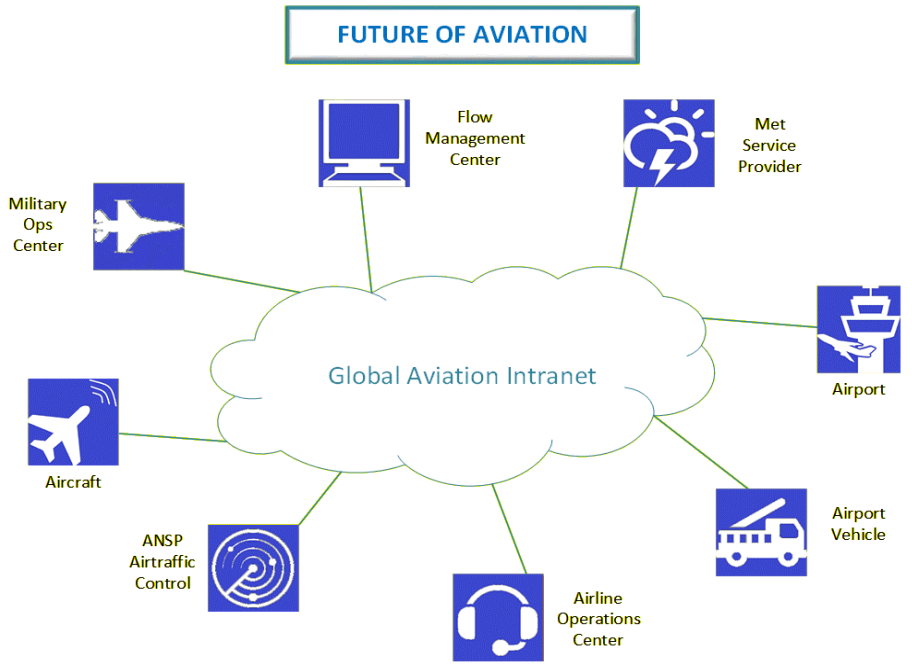
Fit for purpose network evolution to GRAIN



- Specific systems and networks
- Point to point communication
- Physical infrastructure
- Low connectivity
- Limited Automation with user oversight

=

Low exposure
Limited impact



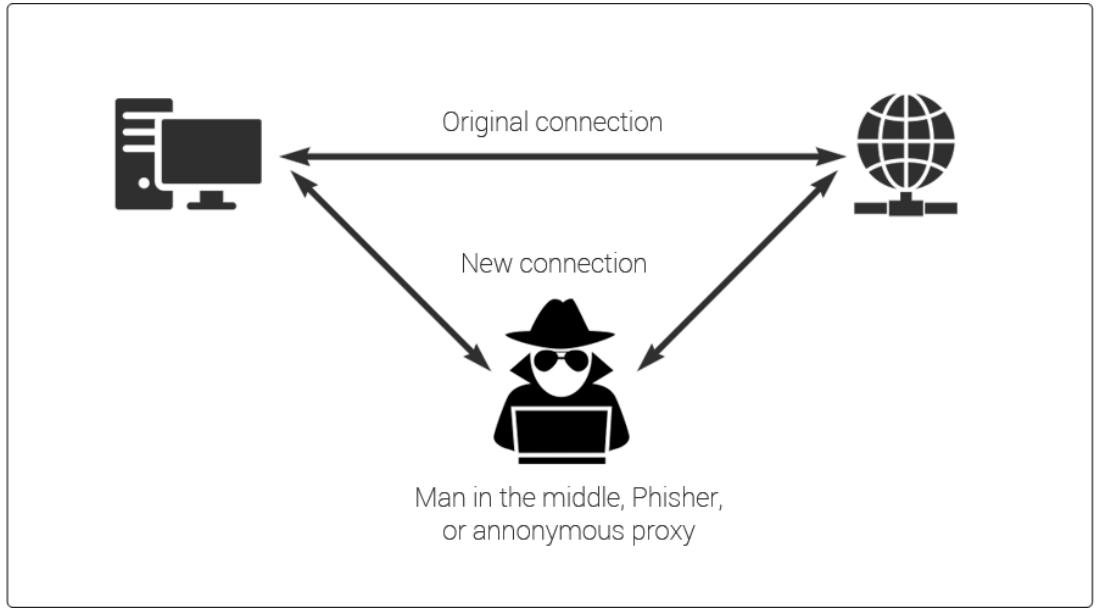
- Multi-stakeholder system of systems
- Public networks
- Increased use of COTS and standard protocols
- Virtual infrastructure
- High connectivity
- Increased Automation with minimum user oversight

=

High exposure
High impact

Man in the Middle (MITM) Attacks: a GRAIN Trust Threat

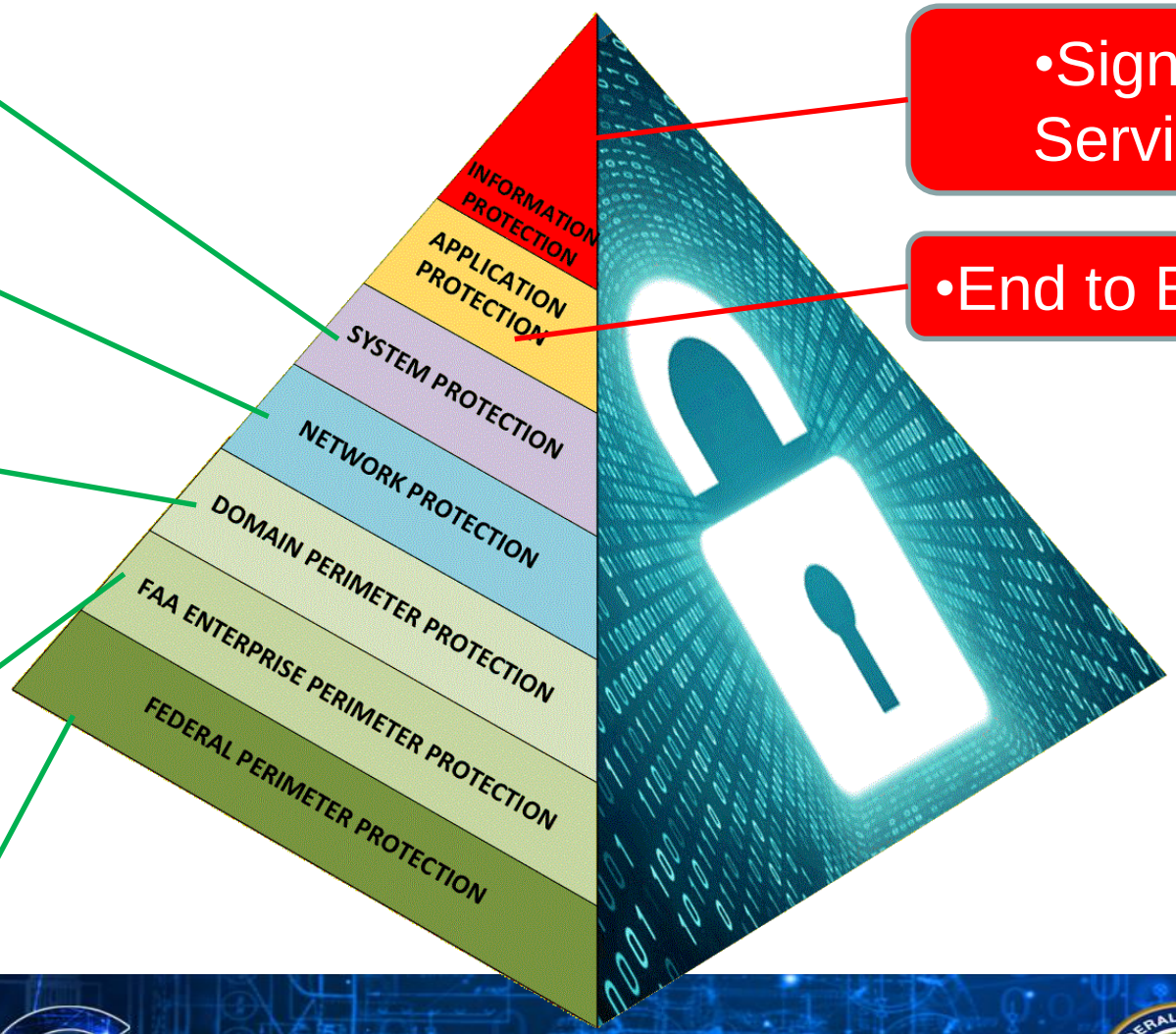
- **Man-in-the-middle(MITM) attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation**
- **The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected party**
- **A MITM attack allows the 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)**

Limited MITM protection with traditional controls

- Malware, Software, system configuration protection
- Virtual Private Networks protection
- NAS Enterprise Gateway protection
- “Trusted Internet Connection” (TIC) protection
- DHS Internet protection



- •Signing as a Service (Sa^2)
- •End to End security

Two distinct technical approaches: Connection vs. Message oriented exchange

Connection oriented exchange – application security

- **Two applications negotiate a connection over the network.**
- **The applications can perform mutual authentication**
- **The applications can verify each others identity**
- **The applications can verify the integrity of the exchanged information**

Message oriented exchange – Information security

- **The Producer application of the information doesn't know the consumer application**
- **The Producer can add a security header to the information, authenticating itself and protecting the integrity of the information**
- **The consumer can verify the authenticity and integrity of the information**

Signing as a Service (Sa^2) and Verifying as a Service (Va^2) for message oriented exchange

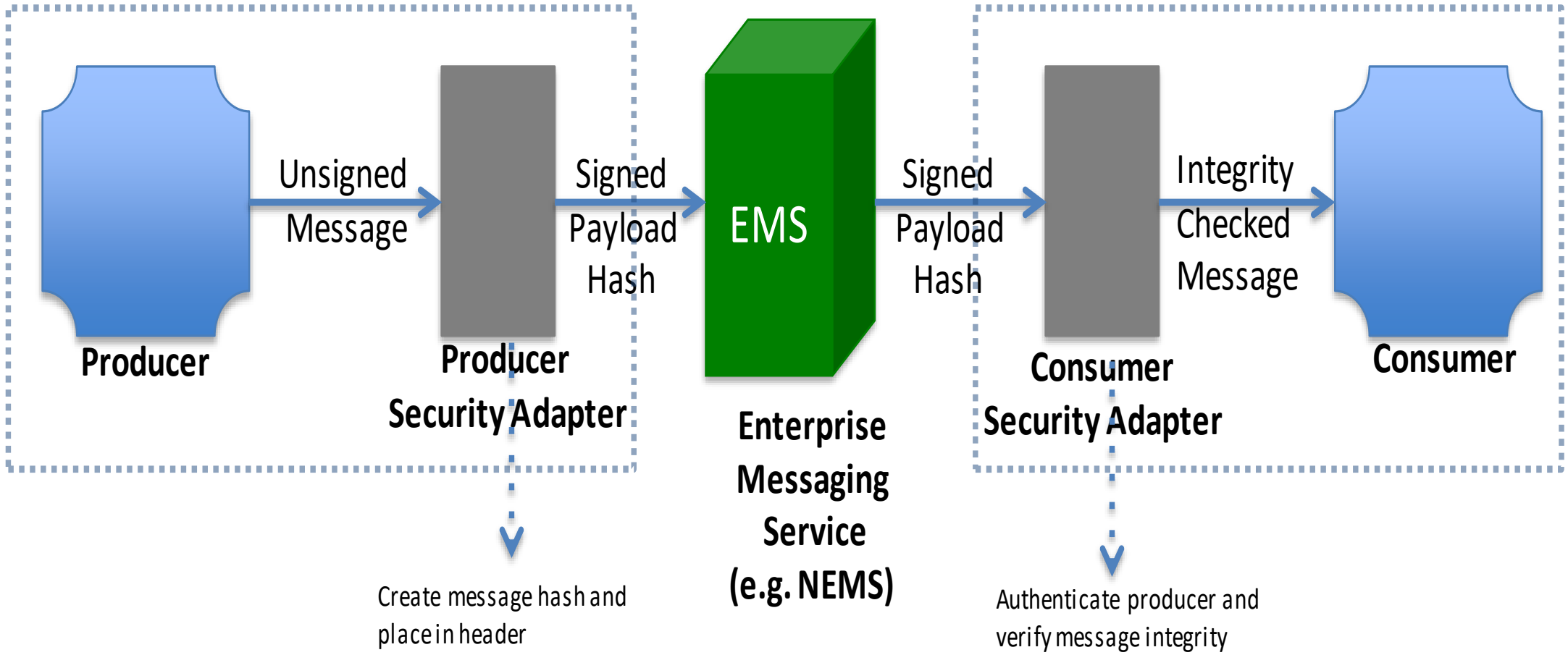
Signing as a Service (Sa^2)

- **Adds the identification of the producer to the information**
- **Adds a cryptographically secure signature to the information, protecting the integrity of the information**
- **Acts on behalf of the producer or is integrated in the producer**

Verifying as a Service (Va^2)

- **Verifies the trust worthiness of the producer identification**
- **Verifies that the information has not been modified between the producer and the consumer**
- **Acts on behalf of the consumer or is integrated with the consumer**

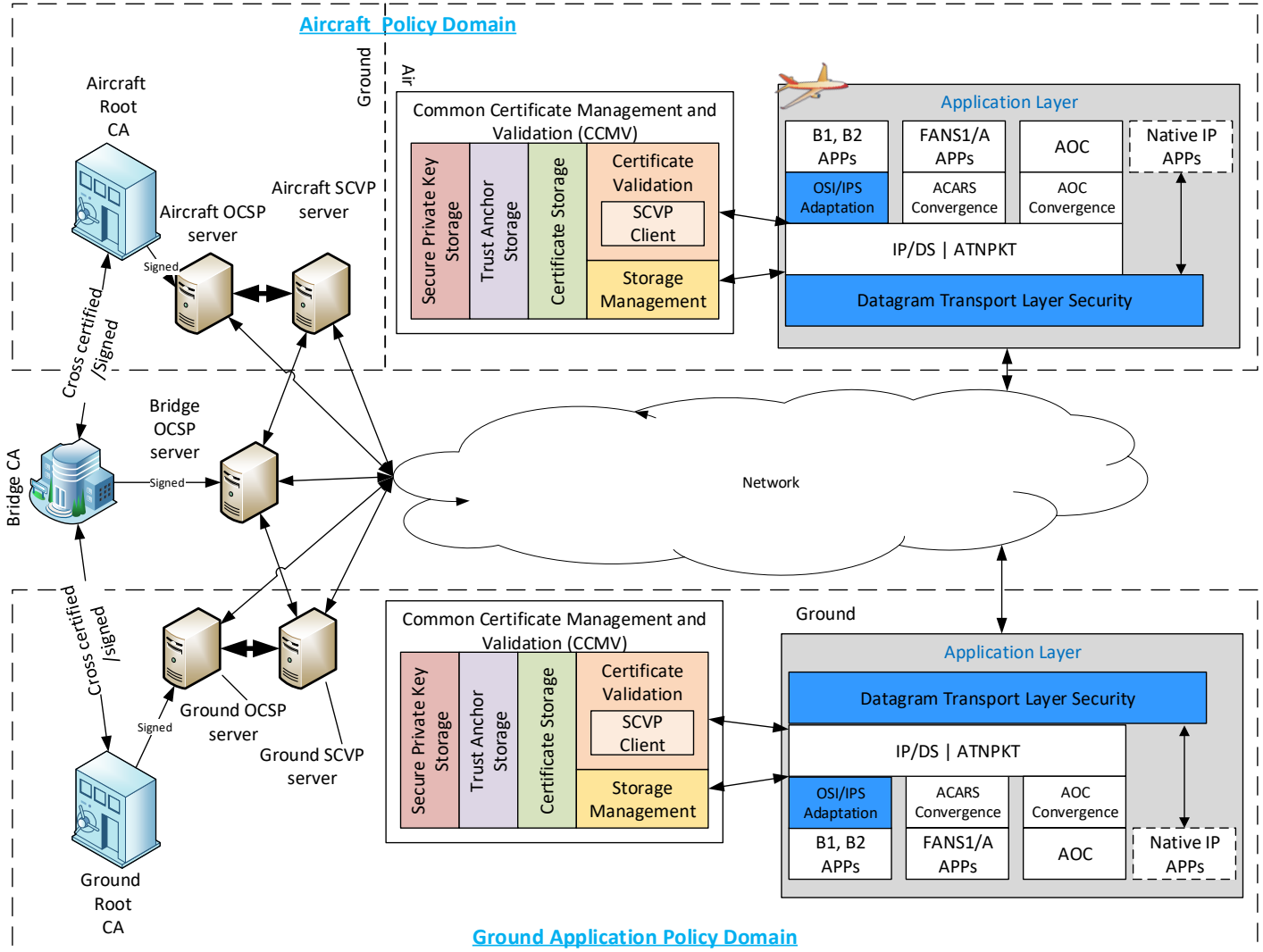
Sa² and Va² SWIM JMS Scenario



Connection oriented exchange: Datagram Transport Layer Security (DTLS) for DataCom

- **DTLS is a standard IETF protocol supported by Internet Protocol Services**
- **DTLS creates a secure communication session between two applications**
- **DTLS performs mutual authentication using public key infrastructure**
- **DTLS supports low overhead symmetrical encryption of integrity signatures without payload encryption**
- **DTLS can support payload encryption if needed**

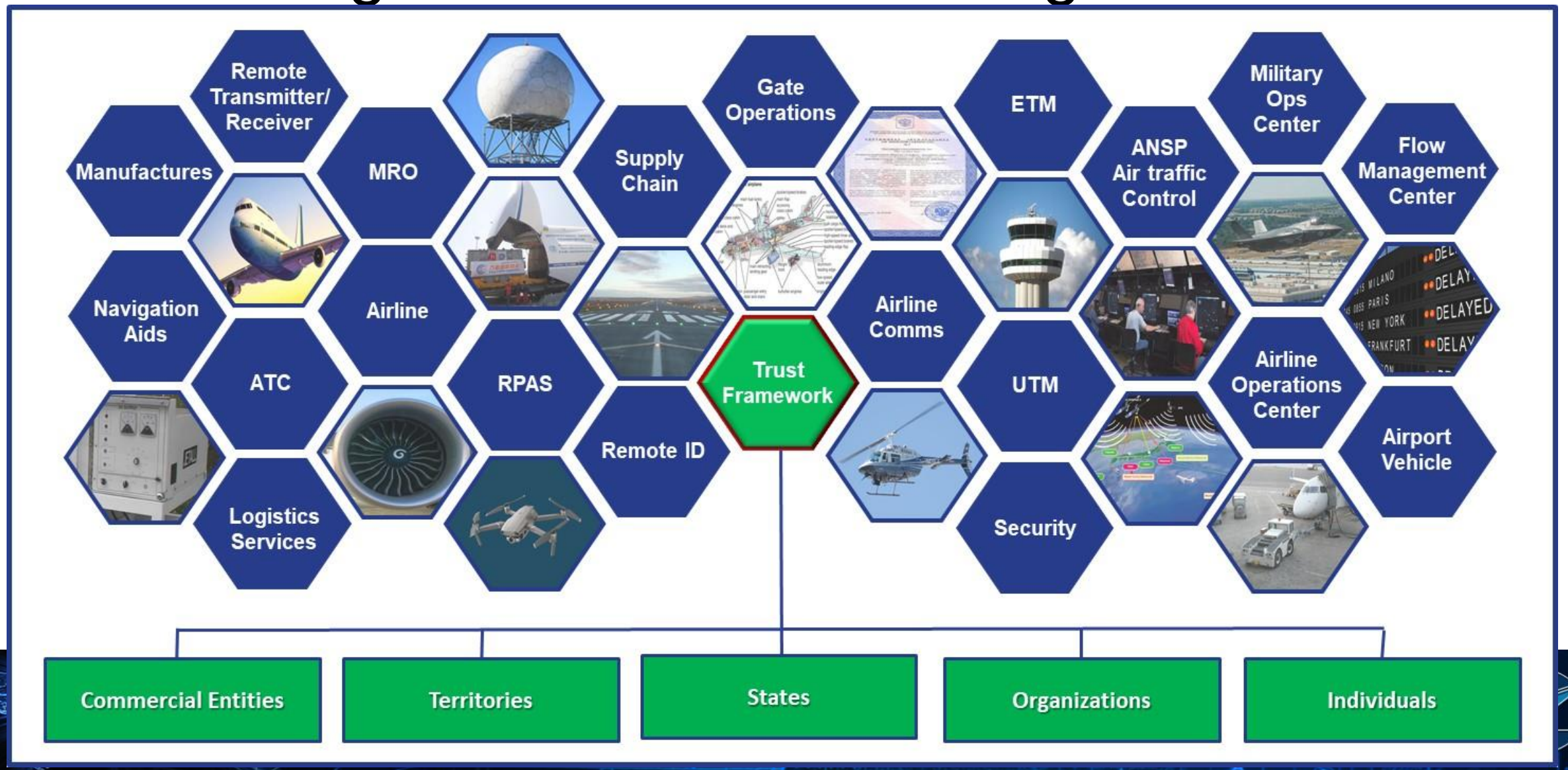
DTLS for DataCom



Authentication in an international context

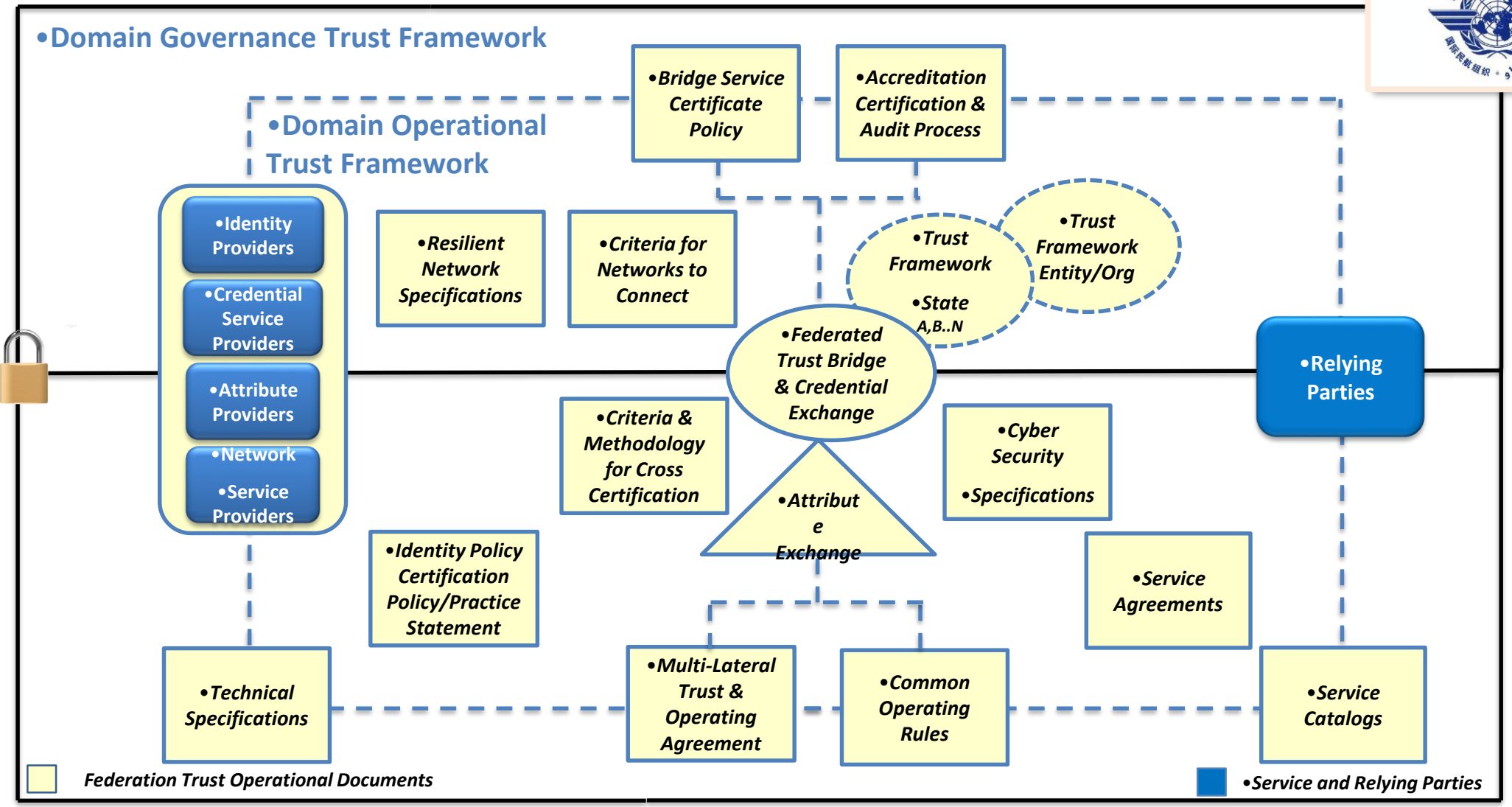
- **Traditionally each organization and each country issues their own digital identities**
- **The issuance of the digital identity requires a sufficient level of vetting and proofing of the person or sponsor (device identity)**
- **In order for mutual or origin authentication to work, different organizations and countries must recognize and trust each others digital identities**
- **The ICAO global Trust Framework will provide the legal, policy and governance framework to ensure that members of the trust framework can recognize and trust each others digital identities**

Common Need Across the Ecosystem…
Establishing Trust and Maintaining Trust



ICAO Domain Trust Framework

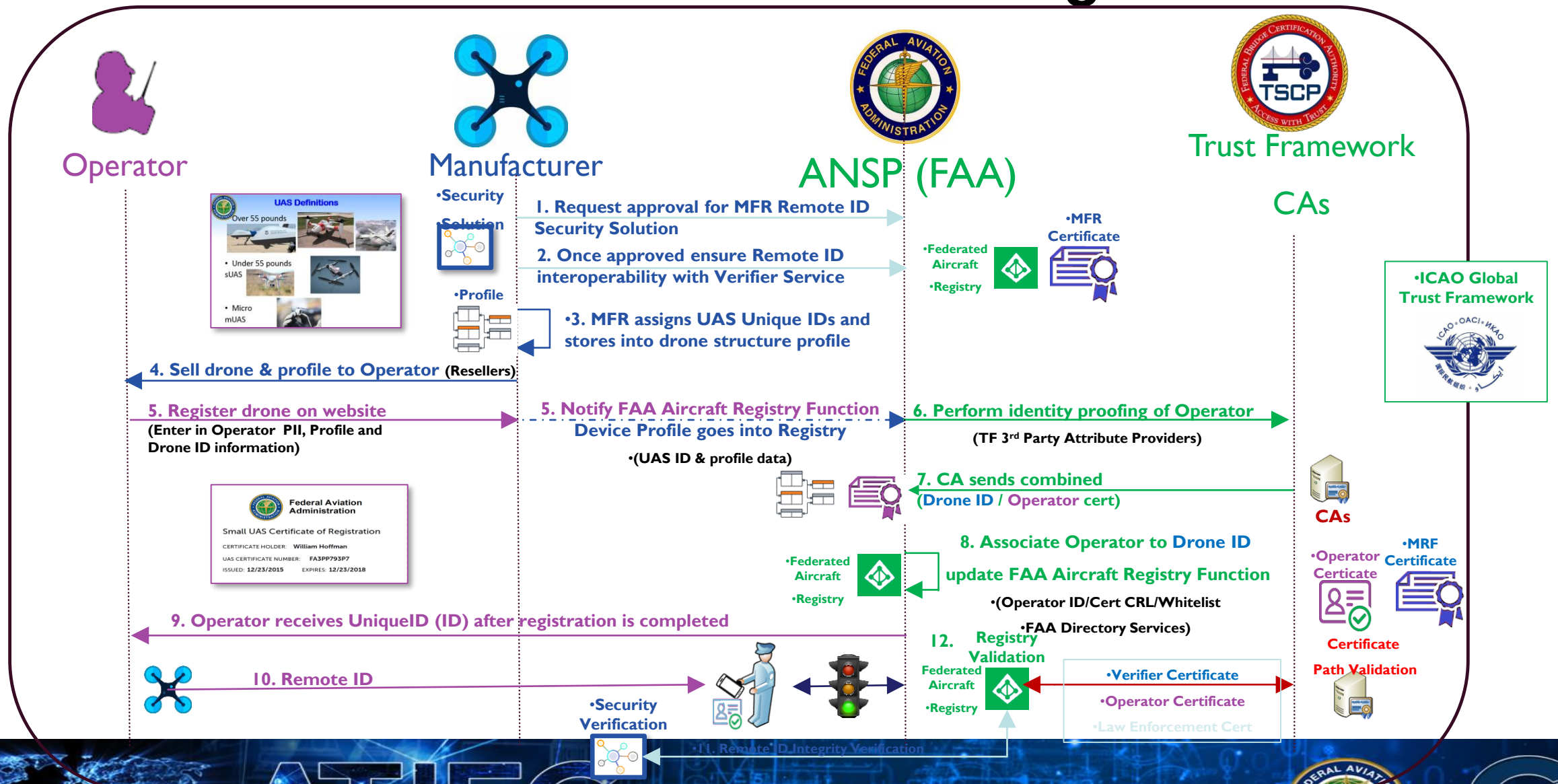
ICAO Global Trust Framework



International interoperable digital identities

- **The ICAO Global trust framework provides the ability to exchange and trust identities across organizations and countries**
- **The actual implementation of the global trust needs to be established through a trust anchor allowing relying parties to establish trust and verify the validity of the exchanged identities**
  - Use of a Bridge Certificate Authority with Server Certificate Validation Protocol (SCVP) servers
  - Use of Trust lists, per domain stored in a SCVP server

ASTM F-38 Secure Remote ID through Sa² and Va²



ASTM F-38 Secure Remote ID (continued)

- Enables law enforcement to distinguish “Friend” from “Foe”
- Each manufacturer can provide their own solution without the standard dictating what algorithm to use
- Algorithms can evolve without breaking the concept
- Standardized API guarantees interoperability and future compatibility
- The Globally federated aircraft registry provides a secure international digital trust anchor for pilot, operator, owner and aircraft within the ICAO Global trust framework for UAS and traditional aviation

Questions

Rob Segers,
NextGen ISS Architect