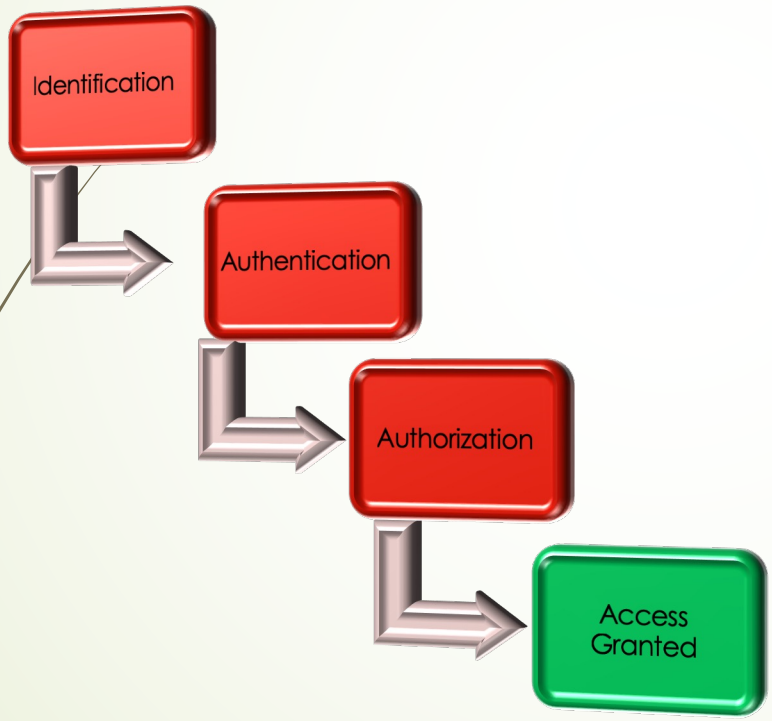
Secure Airspace for UAM Workshop: *Identity and Access Management*

Adam Monsalve (CNA) and Robert Segers (FAA)

Outline

- What is IAM?
- Importance of IAM in UAM
- IATF and Trust
- Federated vs. Centralized Identity in UAM
- Poll Question
- Q&A

What is Identity and Access Management?



- IAM
  - Security discipline which ensures that only the correct entities have access to the correct resources at the correct times
- Key Security Concepts in IAM
  - **Identification** – differentiating a specific user from other users
  - **Authentication** – verifying the identity of a user, service, application, system,
  - **Authorization** – allowing a user to access a resource based on their permissions

Identity in UAM

- UAM will consist of a myriad of resources and users, each of whom require access to certain elements of UAM
  - Vertiport operators require access to certain resources while managers of the DSS require access to different resources
- The ability to apply IAM principles and technologies to UAM will ensure that all resources are adequately protected
- IAM applies to both human users (e.g., RPIC) and non-person entities (e.g., PSU servers)

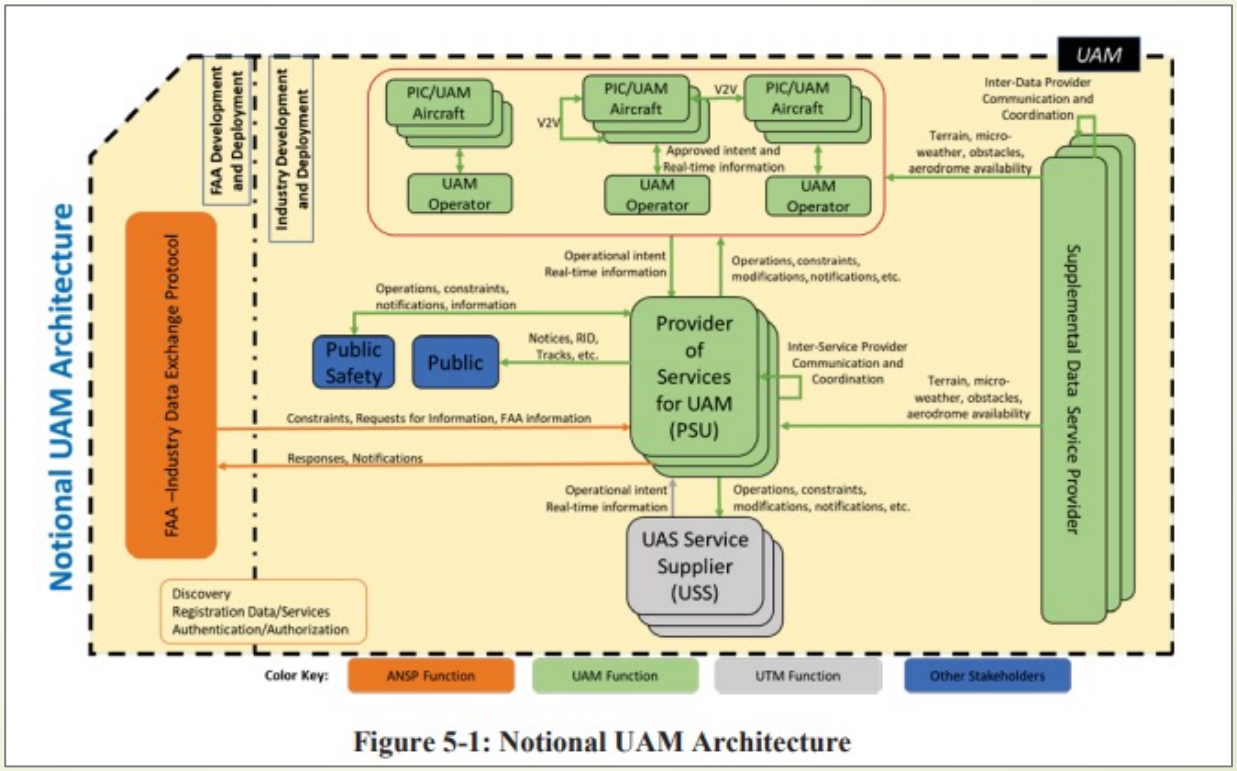
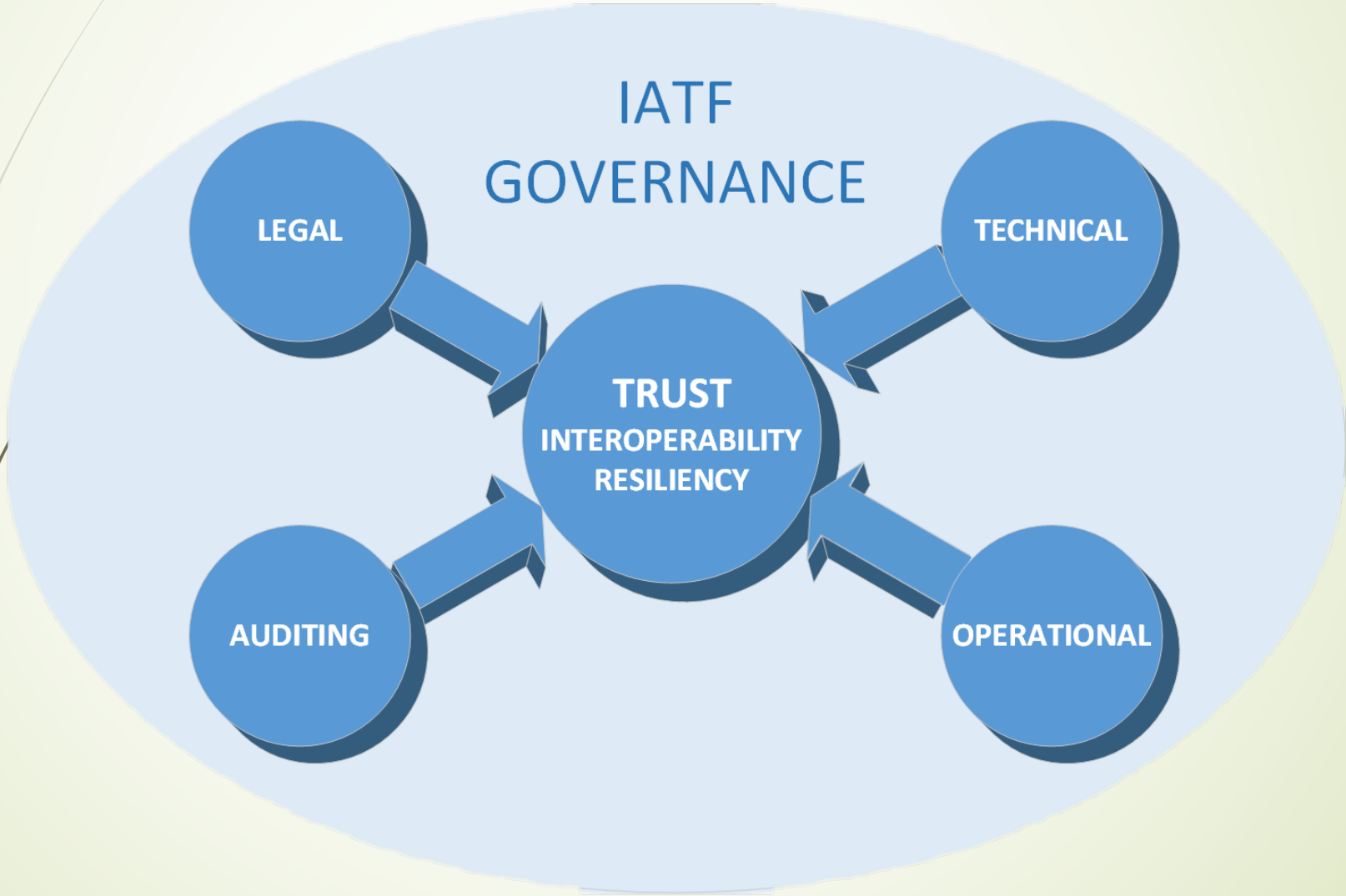


Figure 5-1: Notional UAM Architecture

Establishing Trust: International Aviation Trust Framework (IATF)

International Aviation Trust Framework (IATF)



How does IAM secure UAM?

- Properly implemented IAM security will help to prevent numerous potential cyber threats

Spoofing

Attackers can falsely identify as another entity; such as a UAM aircraft, Provider of Services for UAM (PSU), or other UAM entity

Data Leakage

Without IAM implemented properly, privacy, proprietary, and national security information could be released to the incorrect entity

Denial-of-Service

IAM security controls can help to prevent DOS attacks by making it more difficult for attackers to access UAM systems

Spoofing

Attackers can falsely identify as another entity; such as a UAM aircraft, Provider of Services for UAM (PSU), or other UAM entity

Malicious actors can spoof a vertiport to cause incidents, posing a safety risk

UAM participants could use spoofing to favor themselves in favor of competitors

https://www.flightglobal.com/business-aviation/skyports-readies-worlds-first-vertiport-for-evtol-aircraft/134184.article

Data Leakage

Without IAM implemented properly, privacy, proprietary, and national security information could be released to the incorrect entity

The UAM ecosystem will contain significant amounts of sensitive data, which IAM controls are needed to adequately protect

https://eveairmobility.com/

Denial of Service (DOS)

IAM security controls can help to prevent DOS attacks by making it more difficult for attackers to access UAM systems

https://www.nasa.gov/aero/taking-air-travel-to-the-streets-or-just-above-them/

IAM in UAM: Federated or Centralized?

- Two different approaches may be applied to UAM: Centralized vs. Federated IAM
- Centralized IAM
  - Entities in UAM are all managed by a central actor who ensures that each entity applies the appropriate access controls prior to access UAM resources
  - Potential improved security, but more challenging to scale; burdensome on managing entity
- Federated IAM
  - Entities within UAM manage the identities of their own respective users
  - Increased scalability; requires establishment of trust across federated actors

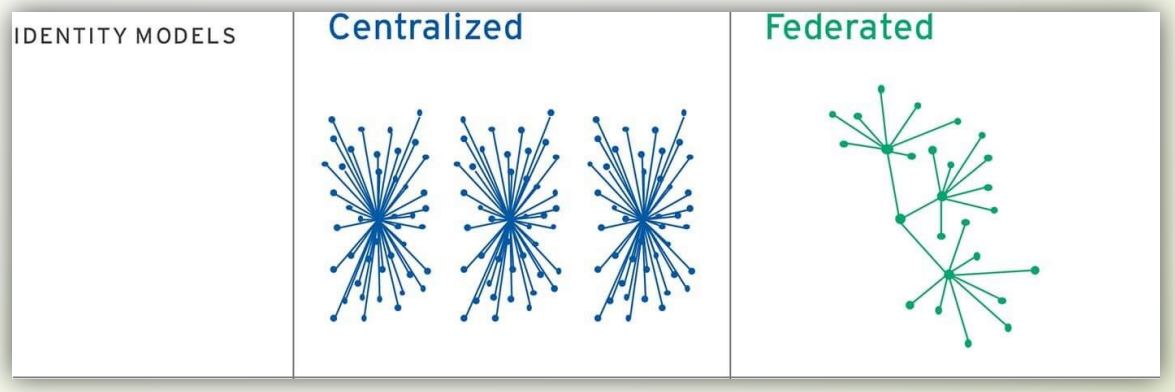


Image Source: https://www.citi.com/ventures/perspectives/opinion/digital-identity.html