MAAP UPP2 Final Report Attachment A

Security Considerations for Operationalization of UTM Architecture

January 12, 2021

1. Introduction

This paper documents the results of an analysis of security considerations for operationalization of the Unmanned Aircraft System (UAS) Traffic Management (UTM) ecosystem. This analysis was performed by the Virginia Tech Mid-Atlantic Aviation Partnership (MAAP) UPP2 team, including industry representatives from AirMap, AiRXOS (part of GE Aviation), ANRA, Wing, and Google as well as FAA and NASA security representatives.

The goals of this analysis were to:

a. Identify threats, risks and impacts
b. Identify unique challenges with the ASTM UTM Interoperability standard assuming a nominal level of security controls and a Security Risk Management Plan (SRMP). ISO27001 was accessed as an assumption for nominal level of security and process controls.
c. Define a plausible UTM attacker profile
d. Identify additional critical controls and gaps in the standard
e. Generate this report as an input to the ASTM working group for the UTM Interoperability standard

The topics addressed in this paper include the following:

a. Risk analysis framework
b. Context for UTM ecosystem
c. Adaptation of the risk analysis framework for this analysis
d. Analysis of UTM scenarios
e. Analysis of FAA/NASA-generated protection needs
f. Definition of an Attacker Profile considered for the threat scenarios
g. Review of ICAO Aviation Trust Framework (IATF)

2. Reference Documents

The following documents are either referenced by this document or provide relevant background information.

- Rios, Joseph L., Smith, Irene, Venkatesen, Priya. NASA/TM-2019-220364, *UAS Service Supplier Framework for Authentication and Authorization - A federated approach to securing communications between service suppliers within the UAS Traffic Management system*, September 2019. https://utm.arc.nasa.gov/docs/2019-UTM_Framework-NASA-TM220364.pdf

  This document provides NASA's UTM Research perspective on Authentication and Authorization within the UTM ecosystem.

- Rios, Joseph L., et al. NASA/TM-2019-220024, "UTM UAS Service Supplier Development, Sprint 1 Toward Technical Capability Level 4, 2018. https://utm.arc.nasa.gov/docs/UTM_UAS_TCL4_Sprint1_Report.pdf

  This document captures test results from TCL4 where the authentication and authorization approach was tested.

- ASTM UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability Draft Technical Standard v0.2.

  This document was used to establish the context for the operational environment and to identify interoperability interfaces for which failure scenarios needed to be defined. This document is not yet published but can be reviewed by participants in ASTM Working Group 63418

- ASTM F3178-16, Standard Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS), 2016.

  This practice provides a standardized framework for operational risk assessment. Elements of this document were used or tailored for this activity.

- ICAO Aviation Trust Framework

  Documentation for the ICAO Aviation Trust Framework has not yet been published for general consumption. Interested parties should contact the ICAO Air Navigation Bureau or a member of the Trust Framework Study Group (TFSG).

- ISO/IEC 27001:2013, Information security management systems — Requirements (second edition), 2013.

This is an international standard that sets out the specification for an information security management system (ISMS).

- ISO/IEC 27005:2018, Information Security Risk Management

  This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. This document was used to guide the risk analysis process for this activity.

- NIST Special Publication (SP) 800 Series

  This series of documents published by the United States National Institute of Standards focus on Computer/Information Security. Among other topics, they also address a risk analysis framework similar to ISO 27005.

- RFC 7519, JSON Web Token (JWT), 2015.

  This document is a product of the Internet Engineering Task Force (IETF). Per RFC 7519, "A JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted." https://tools.ietf.org/html/rfc7519

- RFC 6749, The OAuth 2.0 Authorization Framework, 2012

  This document is a product of the IETF. Per RFC 6749, "The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849." https://tools.ietf.org/html/rfc6749

  OAuth 2.0 is used in Interoperability APIs in the ASTM UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability Draft Technical Standard v0.2.

.

3. Analysis Process Overview

Figure 3-1 illustrates a generic risk analysis framework based on the ISO 27005, Risk Management Standard, and the NIST SP800 series of security standards. This framework was used to structure the analysis performed by the MAAP UPP2 team.

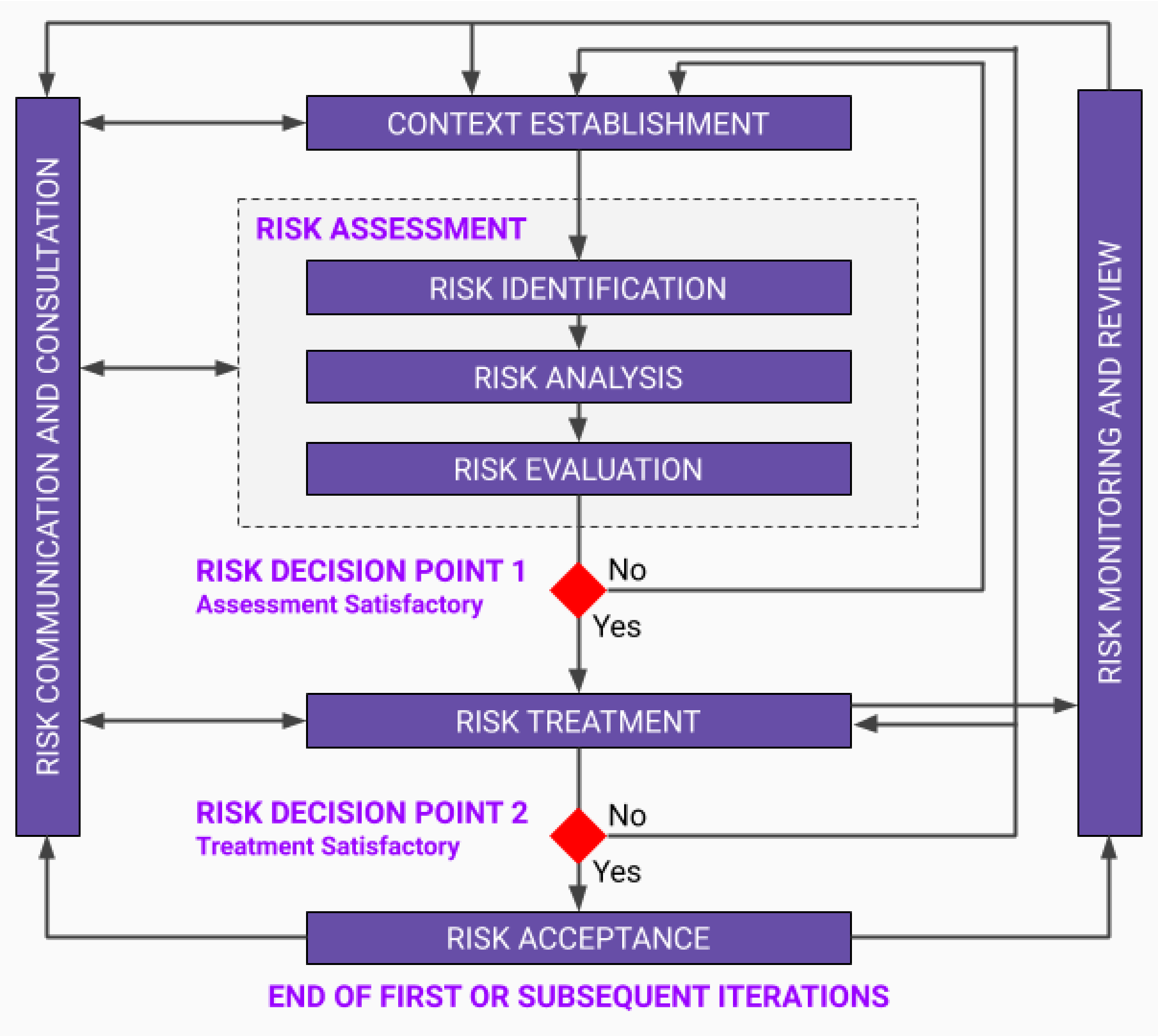


Figure 3-1. Risk Analysis Framework Based on ISO27005 and NIST SP800

The main flow of the process proceeds from top to bottom in the middle of the figure.

a. Context Establishment includes:
   i. Documenting system boundaries, the system architecture, roles and responsibilities, and relevant assumptions
   ii. Identifying in the system architecture what is trusted and what is not trusted, e.g.:
      1. Maintenance personnel are trusted
      2. Aircraft in the vicinity are not trusted
   iii. Defining the platform, including:
      1. Untrusted components such as internet facing systems
      2. Trusted components such as other USSs

iv. Partitioning the platform into trust domains, including untrusted, trusted, and intermediate trusted

v. Establishing the attacker profile (e.g., Amateur, Layman, Proficient, Nation State)

Context establishment for this analysis is documented in Section 4.
The Attacker Profile is documented in Section 5.

b. Risk Assessment includes

i. Risk identification and risk analysis, which produces a list of threats and risks

ii. For each threat and risk, risk evaluation is performed to calculate risk. This involves:

1. Characterizing the likelihood of the risk and the impact of the risk.
2. Establishing the inherent risk (before any compensating controls are applied); this is typically a combination of the risk and impact.
3. Identifying compensating controls that are recommended or required

The risk assessment for two different sets of scenarios, including methodology specifics, and documented in Section 6.

c. After Risk Assessment is performed, the first key decision point is whether the assessment provides an adequate basis for proceeding to Risk Treatment. If not, the process iterates by returning to the Context Establishment step and repeating the Risk Assessment based on updated context. If the assessment is adequate, the process proceeds to Risk Treatment.

d. Risk Treatment involves recalculating the risk after mitigations have been applied to determine if the mitigations result in an acceptable residual risk.

e. After Risk Treatment is performed, the second key decision point is whether the residual risks are acceptable. If so, the process completes. If not, the process iterates by returning to earlier steps, which could include Risk Treatment or back to Context Establishment.

f. Given a set of acceptable residual risks, the system can be deployed with two processes that support iteration as necessary:

i. Risk Monitoring and Review involves the ongoing monitoring of the system and review of collected data to determine if there are circumstances that warrant a return to the Context Establishment or Risk Treatment steps.

ii. Risk Communication and Consultation involves keeping abreast of new risks and mitigation techniques that may not yet have been encountered through monitoring, but nonetheless require iteration.

4. Context Establishment

To establish the context for the Risk Assessment a High Level overview of the UTM ecosystem for Strategic Conflict Detection and Constraints was provided in Figure 4-1. This figure from the working draft of the UTM Interoperability specification being developed under ASTM Working Group WK63418 was used as a baseline for a security domain model assessment.

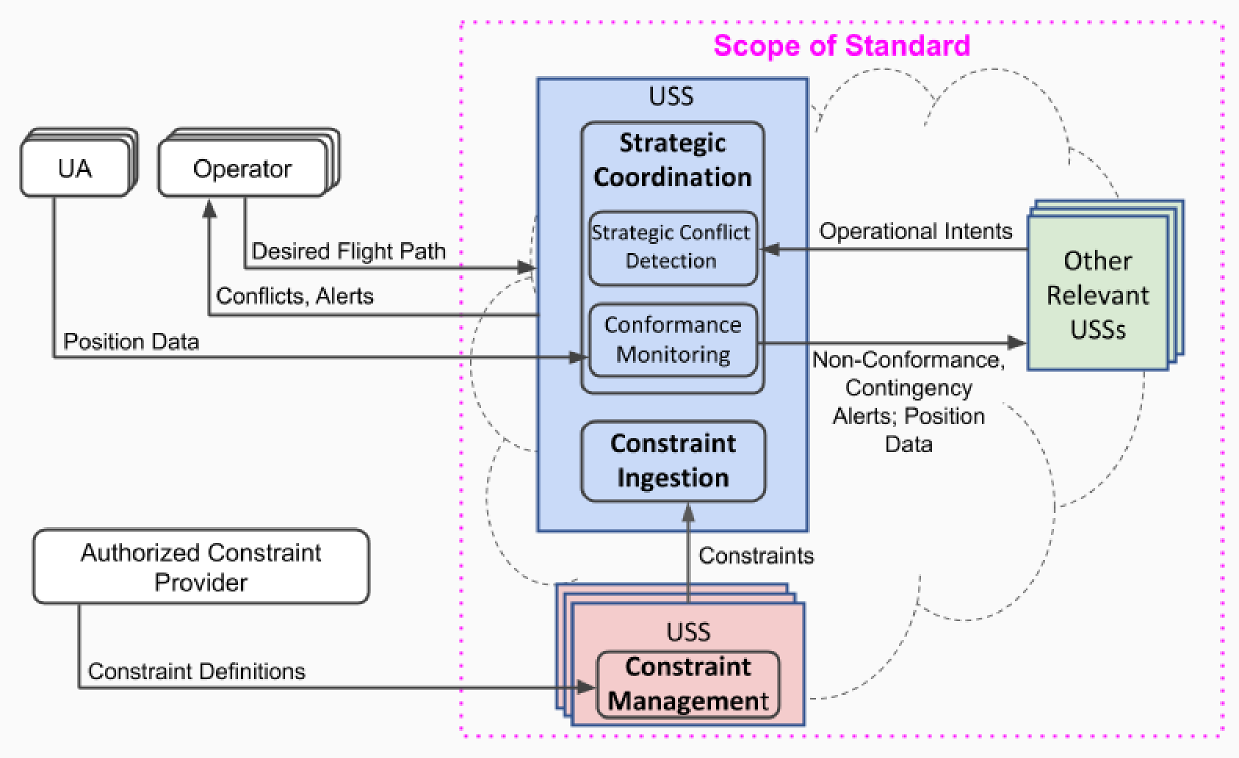


Figure 4-1. Overview of Strategic Coordination and Constraints

Three distinct roles (e.g. privileged domains) for USS are defined in the draft standard and are indicated by bold text in Figure 4-1. They include Strategic Coordination, Constraint Management and Constraint Ingestion. Strategic Coordination includes detection of conflicts between operational intents or between operational intents and constraints. In some cases, operational intents are owned by Other Relevant USSs, and they must share the operational intent data when requested from another USS performing Strategic Coordination. Strategic Coordination also includes Conformance Monitoring, which monitors position data for UAS to verify if the aircraft is staying inside its planned operational intent. Constraint Management enables the creation of constraints and sharing of constraint information with USSs. Constraint Ingestion allows USSs that need constraint information to ingest the data.

Figure 4-2 overlays Figure 4-1 with security trust domains.

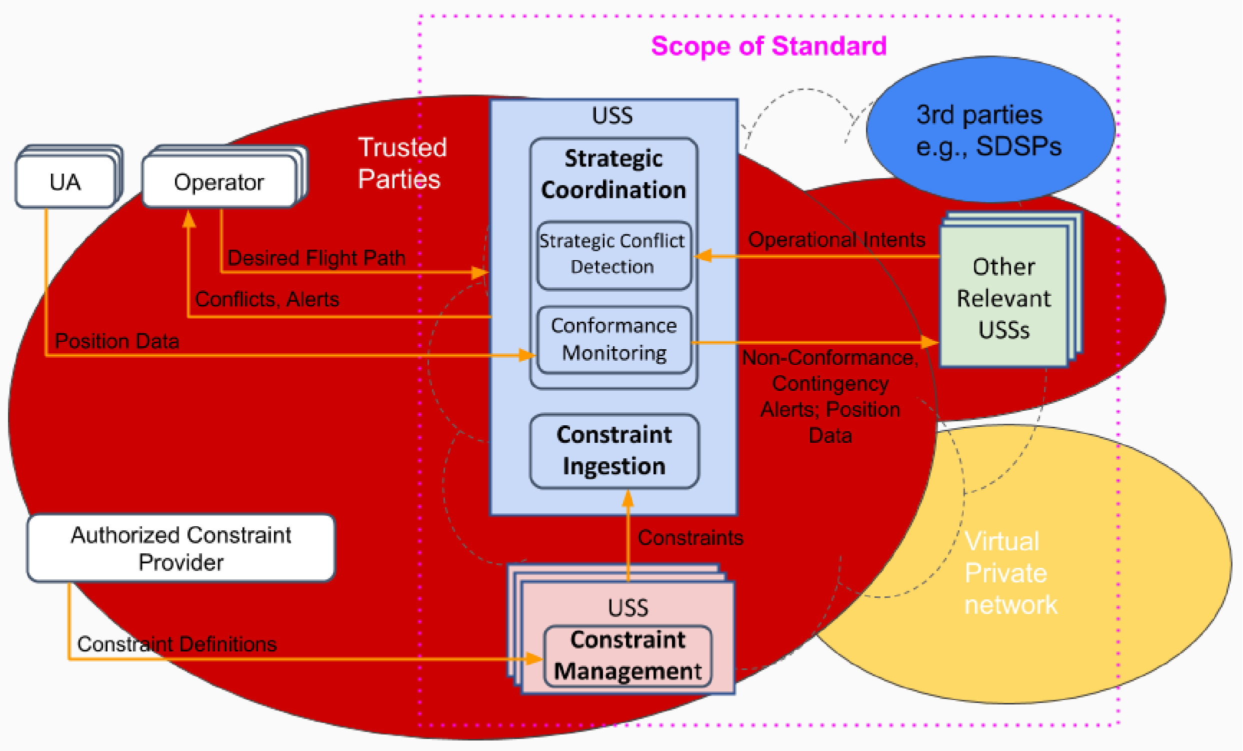


Figure 4-2. Domains for Strategic Coordination and Constraints

To establish the context for the given roles in the critical attack paths, three security domains were chosen to capture the trust model around first and third parties involved in the standard.

1. Trusted Parties - These include the USS Operators/Providers which have access to the UTM network and provide critical functions such as strategic coordination and constraint management. It is anticipated that USSs will undergo an onboarding process administered by the applicable regulator in order to become a trusted party. (The trust validation of this process could be based on the ICAO Trust Framework). The onboarding process would verify that a candidate USS adheres to operating rules established by the regulator, including cyber-related rules. Successful onboarding results in the USS being granted credentials that can be used to request tokens to authenticate as necessary to interact with other trusted parties.

2. Intermediate trusted Parties - These receive access through Virtual Private Networks and authenticated services. These could include SDSPs providing services to USS. Providing access to the Virtual Private networks would undergo specific onboarding procedures.

3. Other 3rd Parties - These have defined interfaces through 3rd party security controls in order to interface with the USS critical functions. They could also include SDSPs or other services on the internet.
    a. Per current FAA environment, these would be consumers of data, through appropriate controls, may include service authentication

If entities are not part of domain group 1-3 they will not receive access unless explicitly granted.

Note for the analysis documented in this white paper, there are no defined entities in the Intermediate Trusted Parties or Other 3rd Parties security domains. This analysis will be revisited if and when entities in those trust domains are added.

5. Attacker Profile

An attacker profile is a characterization of the goals, motivations and capabilities (technical and monetary) of cyber threat actors. The characterization of attacker capabilities heavily influences the security controls required in a system.

Multiple categorizations of attacker profiles can be found in literature. For example, one model includes pranksters, hacktivists, super-criminals, and nation-state attackers. Another model includes recreational, criminal, hacktivist, organized crime, and state sponsored. The common thread through the different models is the technical sophistication and resources available to the attacker increase as the model approaches nation-state actors.

For this analysis, the group defined the attacker profile as follows. This in turn set the bar for countermeasures and mitigations.

- Proficient Attacker
    - Access to public vulnerabilities
    - Able to research and identify new vulnerabilities
    - Able to carry and coordinate attacks
        - but not state sponsored attacks
- Funding:
    - Access to a max of 10 million dollar budget
- Access:
    - Access to external interfaces which can escalate to access to internal interfaces through phishing and trojans
    - Stolen Documentation
    - Capable of successful attacks on internet facing systems
- Skills:
    - Network penetration testing
    - Reverse Engineering applications
    - System exploitation

Given our assessment, we do not consider nation state attackers and capabilities the level of attacker profile the platform is standardized for. As such, breaking cryptographic functions and protocols like TLS would be considered unlikely entrance vectors for successful attacks.

Attacker capabilities have been defined on the assumption that external and internal parties could mount a successful attack which could negatively affect a single function or operation in the platform. This analysis would need to be revisited for increased attacker capabilities, such as multilateral or nation state actors attacking the platform simultaneously on multiple paths.

6. Analysis of UTM Threat Scenarios

6.1. Draft ASTM Standard for USS Interoperability Interfaces

6.1.1. Overview

The first analysis of UTM threat scenarios focused on USS-DSS and USS-USS interfaces defined in the draft ASTM standard for USS Interoperability. These interfaces represent the adaptation of the ASTM interoperability paradigm to support the Strategic Coordination and Constraint Management/Ingestion services. They are generically represented in Figure 6.1.1-1.

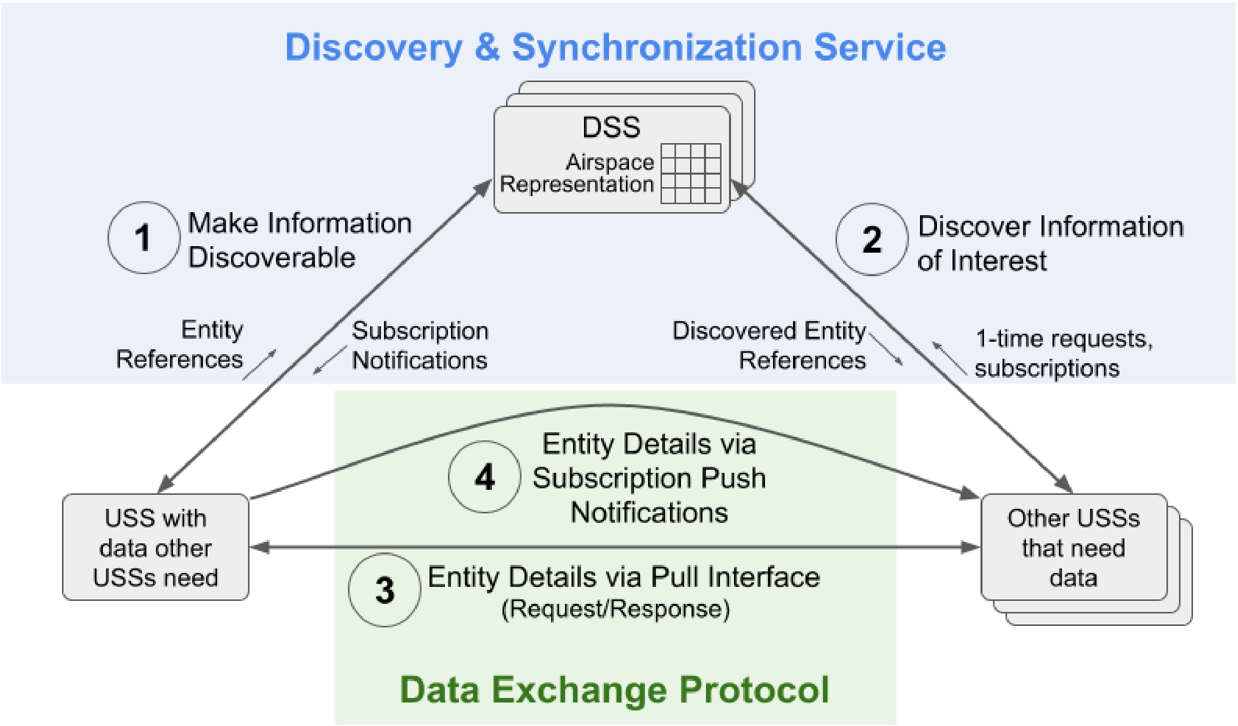

Discovery & Synchronization Service
DSS
Airspace Representation
1 Make Information Discoverable
2 Discover Information of Interest
Entity References
Subscription Notifications
Discovered Entity References
1-time requests, subscriptions
4 Entity Details via Subscription Push Notifications
USS with data other USSs need
Other USSs that need data
3 Entity Details via Pull Interface (Request/Response)
Data Exchange Protocol

Figure 6.1.1-1. ASTM Interoperability Paradigm.

A USS with data that other USSs may need makes it discoverable by writing an *entity reference* to the DSS (step 1). The entity reference comprises limited information about an *entity,* including where and when the entity will exist and the owner (USS) of the entity. The entity for Strategic Coordination (comprising Strategic Conflict Detection and Conformance Monitoring) is an operational intent -- a set of one or more 4D volumes that define where and when an operation will take place. The entity for Constraint Management and Constraint ingestion is a constraint -- a set of one or more 4D volumes defining where and when a constraint such as a no-fly area will be in effect. The DSS maps entity references into its airspace representation which can logically be thought of as a georeferenced grid.

Other USSs that need the entity data discover the entity references by submitting a query to the DSS (step 2). The query includes the type of entities in which there is interest, and a 4D volume indicating where and when. The DSS maps the query onto the airspace representation and returns a list of intersecting entity references (if any) to the USS.

The USS needing data then uses a peer-to-peer interface to contact the owning USS and obtain the data (step 3). This is a pull interface.

In addition, when a USS makes a query to the DSS, it can put in place a subscription to be notified of new, modified or deleted entity references. When the owning USS updates the DSS with new, modified or deleted entity references, the DSS determines if there are any subscriptions that intersect the entity reference. If so, the DSS informs the owning USS and the owning USS then using the push interface to provide the data to the subscribing USS (step 4).

6.1.2. Methodology

The analysis initially considered the use of ASTM F3178-16 to define impacts (severities) and likelihoods. Table 6.1.2-1 defines the ASTM F3178-16 severities.

Table 6.1.2-1. ASTM F3178-16 Severity Definitions

Severity Level	Definition	Value
Negligible	Little or no negative consequence	1
Minor	Nuisance; minor incident	2
Major	Significant reduction in safety margins; reduction in the ability of pilots to cope with adverse operating conditions as a result of increased workload; serious accident; injury to persons.	3
Hazardous	Large reduction in safety margins; vast reduction in ability to complete duties accurately; single fatality or serious injury; major equipment damage.	4
Catastrophic	Non-sUAS equipment destroyed (such as electrical transmission lines, substation, water treatment facility, and so forth); multiple fatalities.	5

Table 6.1.2-1 provides the ASTM F3178-16 likelihood definitions.

Table 6.1.2-2. ASTM F3178-16 Likelihood Definitions

Likelihood Level	Definition	Value
Extremely Improbable	Almost inconceivable to occur (<10-9)	1
Improbable	Very unlikely to occur (10^-7 - 10^-9)	2
Remote	Unlikely, but possible, to occur (10^-5 - 10^-7)	3
Occasional	Likely to occur sometimes (10^-3 - 10^-5)	4
Frequent	Likely to occur many times (>10^-3)	5

When the Likelihood and Severity values are multiplied together, they produce a risk category. The ASTM F3178-16 risk categories are provided in Table 5.1.2-3.6

Table 6.1.2-3. ASTM F3178 Risk Categories

Risk Score	Category	Definition
1-4	Low	Acceptable without review
5-11	Moderate Risk	May be acceptable with review
12 to 19	High Risk	Shall be mitigated
20 to 25	Very High Risk	Unacceptable

There were three ways the group adapted the ASTM F3178 approach.

The first stems from the difficulty of assigning a meaningful Severity or Impact absent consideration of other safety mitigations present in the operational context for an operation. Aviation exploits layered approaches to safety. As illustrated in Figure 6.1.2-1, strategic deconfliction (one of the UTM services that was a primary focus for this analysis) will be one of multiple safety mitigators. The complete set of safety mitigators will also vary from operation to operation and would be documented in a safety case in accordance with regulator requirements. (One standardized approach uses the Specific Operation Risk Assessment (SORA) guidelines.) The impact of losing any one mitigator varies depending on the other mitigators.

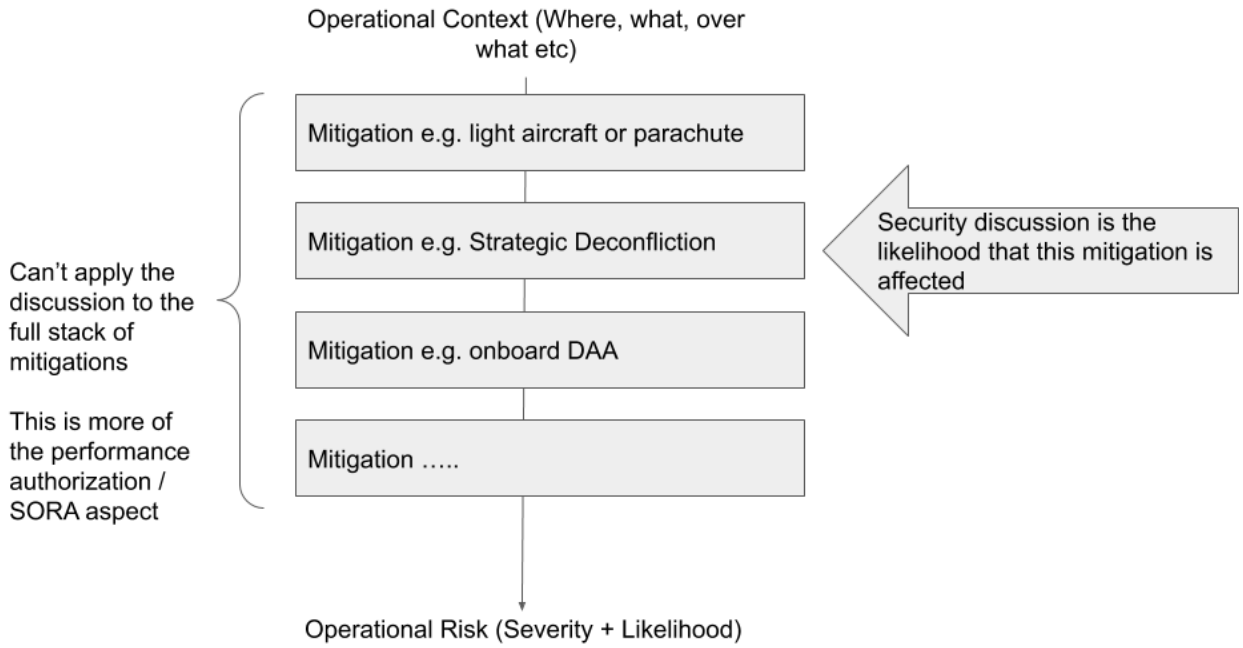

Operational Context (Where, what, over what etc)
Mitigation e.g. light aircraft or parachute
Mitigation e.g. Strategic Deconfliction
Mitigation e.g. onboard DAA
Mitigation …..
Security discussion is the likelihood that this mitigation is affected
Can't apply the discussion to the full stack of mitigations
This is more of the performance authorization / SORA aspect
Operational Risk (Severity + Likelihood)

Figure 6.1.2-1. Impacts for Strategic Deconfliction Security Risks Depends on Additional Mitigations

The group considered an approach where the highest reasonable severity is used. However, it was concluded that this would artificially overstate the severity for all scenarios. Consequently, the group elected to focus on likelihood rather than the combination of Severity and Likelihood.

The second way in which the group modified the ASTM F3178 methodology was to associate cost of successfully carrying out a particular threat with the likelihood level, providing a correlation to the attacker profile. This is summarized in Table 6.1.2-4. (This table became the substitution for Table 5.1.2-2 discussed above.)

Table 6.1.2-4. Cost of Successful Attack Mapped to Likelihood

Likelihood Level	Our quantification of Likelihood Levels (For Highly Efficient Attacker)
Extremely Improbable	Zero-day exploit available; multi-lateral staged attack; 10+ million $ cost
Improbable	1-10 million $ cost; complex mission planning with staff; bot herder, fleet of bots
Remote	Multi-thousand to million $ cost; sophisticated malware (including ransomware, phishing campaign with social engineering)
Occasional	Unsophisticated malware (including ransomware, phishing)
Frequent	Days of effort, free to low cost; includes pay-for-hire tools

Thirdly, the group defined the clip level at which threats are considered acceptable versus requiring further mitigation. This is illustrated in Table 6.1.2-4 by the bolded divider line between Improbable and Remote. Likelihoods above the line (Extremely Improbable and Improbable) were deemed acceptable; likelihoods below the line (Remote, Occasional, Frequent) require mitigation.

In addition to these adaptations of the F3178 methodology, the group also wanted to assess the impact of applying ISO 27001 to the threats. The approach taken was to characterize the control strength of the various areas addressed by ISO 27001 as High, Medium or Low, and then define Likelihood Reduction Value based on the control strength. This reduction value was applied to the likelihood established considering aspects of the draft USS interoperability standard. The characterization of the control strength was performed by Subject Matter Experts in the working group.

The result is summarized in Table 6.1.2-5.

Table 6.1.2-5. Likelihood Reduction Values based on ISO 27001 Control Strength

Strength	Description	Likelihood Reduction Value

High	Controls directly reduce the impact a risk would have or the likelihood that a risk manifests (preventative) Control is applied in a way that minimizes possibility for error (e.g., automation), or is objective Control operates constantly Control has proven efficacy	2
Medium	Controls somewhat reduces the impact a threat would have Controls may detect or catch a risk manifesting early on (detective/monitoring) Controls operate frequently or in regular intervals	1
Low	Controls indirectly affect the risk impact or likelihood Controls are subjective, complex, or efficacy may depend on operator(s) Controls are not well-defined Controls are done at a point in time, with irregular repetition Controls have no proven track record or previous poor result	0

6.1.3. Results

As documented in the attached spreadsheet, under the Scenarios tab, 43 failure or threat scenarios were identified for this analysis. Of the 43, it was determined that no hazard was associated with 16 (for example, airspace might be blocked, but no safety hazard was created). This left 27 scenarios with potential safety hazards.

Of the 27 with scenarios with hazards, 20 were mitigated to a likelihood of improbable or extremely improbable by aspects of the draft standard.

The likelihood of 9 of the 27 were reduced by the addition of ISO 27001 controls, including 2 that were mitigated to the acceptable range of Extremely Improbable to Improbable.

After considering both aspects of the draft standard and the addition of ISO 27001 controls, 4 scenarios had a residual likelihood of Improbable-Remote, all involving a Denial of Service (DoS) attack on a owning USS. The 4 scenarios included:

1. Relevant USS attempts to obtain Operational Intent details from owning USS, owning USS under DoS attack
2. Owning USS attempts to post Operational Intent details to relevant USS in response to subscription notification from DSS, but is under DoS attack
3. Relevant USS attempts to obtain Constraint details from owning USS, owning USS under DoS attack
4. Owning USS attempts to post Constraint details to relevant USS in response to subscription notification from DSS, but is under DoS attack

ISO 27001 includes applicable controls such as Capacity Management and Event Logging, but these controls cannot preclude the possibility of a DoS attack.

6.2. Analysis of NASA-Identified Protection Needs

6.2.1. Overview

As part of their UTM research in 2019, NASA, in conjunction with other government agencies, created a set of protection needs that encompassed industry and government UTM services holistically. The UPP2 team performed a second analysis focused on these protection needs.

For this analysis, the UPP2 team addressed the protection needs that are applicable to industry-provided services, assessing them in the context of the attacker profile described in Section 5. Although there was some overlap with the UTM Interoperability scenarios discussed in Section 6.1, many of the protection needs addressed broader ecosystem management that were not addressed in the first analysis.

The relevant protection needs are provided in the “PNs” tab of the attached worksheet and are described in column B.

6.2.2. Methodology

Because the draft standard currently does not specifically address many of NASA-identified protection needs, the approach of first assessing likelihood based on the standard and then adjusting it based on ISO 27001 controls did not make sense. The spreadsheet does capture whether the standard addresses each protection need, but the analysis focused on assessing each protection need assuming the use of ISO 27001, and identified the key ISO 27001 controls that provide mitigation to achieve an improbable or extremely improbable likelihood.

6.2.3. Results

Applying ISO 27001 resulted in all protection needs (32 in total) being addressed with a residual likelihood of improbable. Key mitigating controls include:

1. Attack and Penetration Testing
2. Security code reviews
3. Static code analysis for security purposes
4. Security Trend and Performance Monitoring (using secure logging and a Security Incident and Event Management (SIEM) system)
5. Implementation of Intrusion Detection and Prevent Systems (IDS/IPS)
6. Message signing
7. Physical security tests
8. Trust Monitoring and Revocation process

9. Use of a protected credentials storage and monitoring for access to keys/tokens and the key-life-cycle (e.g. including monitoring of expiration and revocation status)

7. Recommendations

As the analysis focused on interoperability aspects of the draft UTM USS Interoperability standard, these recommendations assume an implementing organization would encompass domain security controls (system or platform boundaries) providing layer 7 protection for systems and networks outside the security domain.

The analysis described in this paper supports the following recommendations:

1. *The standard should use ISO 27001 as the basis for security requirements.* ISO 27001 is a well-recognized international standard, provides a known baseline for security assessments, and aligns well to the ICAO Aviation Trust Framework (see Appendix B) which may establish additional security controls and process assurance for Suppliers, Operators and Integrators. Through mitigating controls enumerated in Section 5.2.3, ISO 27001 effectively addressed most of the NASA-identified protection needs and appreciably strengthened the residual likelihood of various hazards in the USS Interoperability scenarios.

2. *The standard should mandate UTM ecosystem-wide Security Incident Management and Monitoring with an Integrated Incident Response Plan per ISO 27001.* Most security frameworks (e.g. ISO 27001) require a company to have an Incident Response Plan, as well as a SIEM (Security Information and Event Management) system to monitor anomalies Due to the federated nature of the proposed UTM ecosystem, it is clear that an Integrated Incident Response Plan to coordinate critical issues across USSs would be required.

3. *The standard should include reference architectures with their associated strengths and weaknesses, such as those provided in Appendix A of this document, to provide options for regulators.*

4. *The UTM architecture should assure “fail safe” failure modes of DSS and USS functionality, with appropriate monitoring and notifications, to address residual security vulnerabilities.*

5. *The analysis should serve as a baseline that can be extended/reused in the event new scenarios are identified, key assumptions change, and/or when significant revisions aremade to the USS Interoperability standard.*

Appendix A - Potential Reference Architectures based on key operationalization issues

Based on the identified security controls and threats as part of the UTM Interoperability Threat Analysis the following reference architecture answers the compensating controls for attacks within and outside the architecture to prohibit malicious insider and outsider attacks. There are other architectures that can support the standard, but these have either been deployed or demonstrated with regulators and multiple industry participants. We recommend this information be included in a non-binding appendix to the ASTM UTM USS Interoperability standard.

There are several high level assumptions for the deployments

- There is an onboarding process for approving providers using the integration test environment defined in the standard.
- ISO27001 or equivalent as defined by the standard with potential additional regional requirements
- Message logging and recording as defined by the standard in addition to ISO27001 recording requirements.

The reference architectures below will need further security risk analysis based on the technical implementation of the reference architecture and the implementation of the assumptions above and the minimum performance requirements for identity assurance and key management used by the implementor or mandated by the regulator. This analysis is out of scope of this document since the security risk analysis was focused on interoperability. The identity assurance level will determine the viability of the use of self-signed certificates and the requirements on the self-signer for managing these certificates.

A.1 Base deployment: Access tokens with audience claims

This architecture is being used in Switzerland for the deployment of Network Remote ID. It focuses on establishing the identity and authorization scope of the client USS to the server USS as outlined in figure A.1-1.

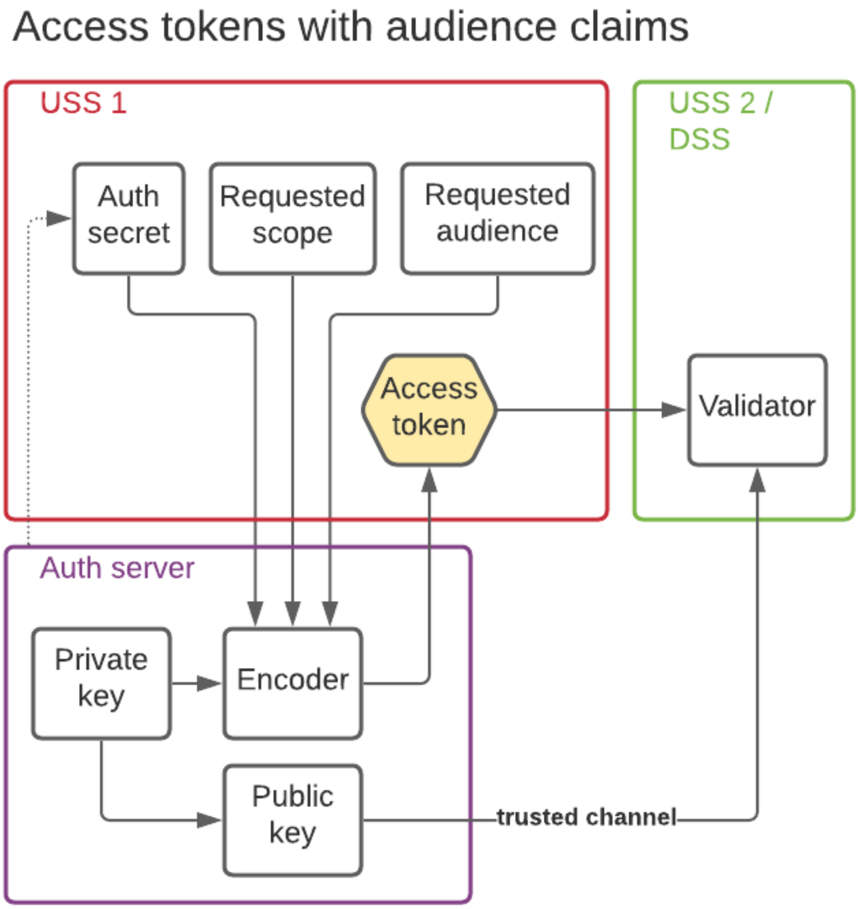


Figure A.1-1. Access Tokens With Audience Claims

Architecture Description:

In this architecture, there is a single resource provider (Auth server) which acts as the authoritative source of truth regarding the services each USS is authorized to provide (authorization scope). A client USS proves its identity and authorization scope to a server within the federated system by providing an OAuth2 bearer access token containing this information along with a cryptographic signature from the Auth server proving its authenticity. The client obtains this token from the Auth server by providing the authentication secret that proves its identity to the Auth server, along with the desired authorization scope the client wishes to assert, and the audience for which this access token is intended. The server validates an incoming access token by checking the token's cryptographic signature with the Auth server's public key. The server must obtain the Auth server's public key, ideally signed by a trusted entity, via a trusted channel to avoid an impersonator substituting their own public key; this is accomplished by requesting the public key from a known domain name using a TLS connection which provides a layer for authentication and encryption to mitigate the risks of an spoofing and impersonation attack between participants in the system.

The audience identifies a particular organization in the federated architecture, and all other organizations within the federated architecture will reject a token for that audience in accordance with RFC 7519. Due to each token specifying exactly one audience, tokens received by one organization in the federated architecture cannot reuse that token to impersonate that client to a different organization in the federated architecture, as is illustrated in figure A.1-2.

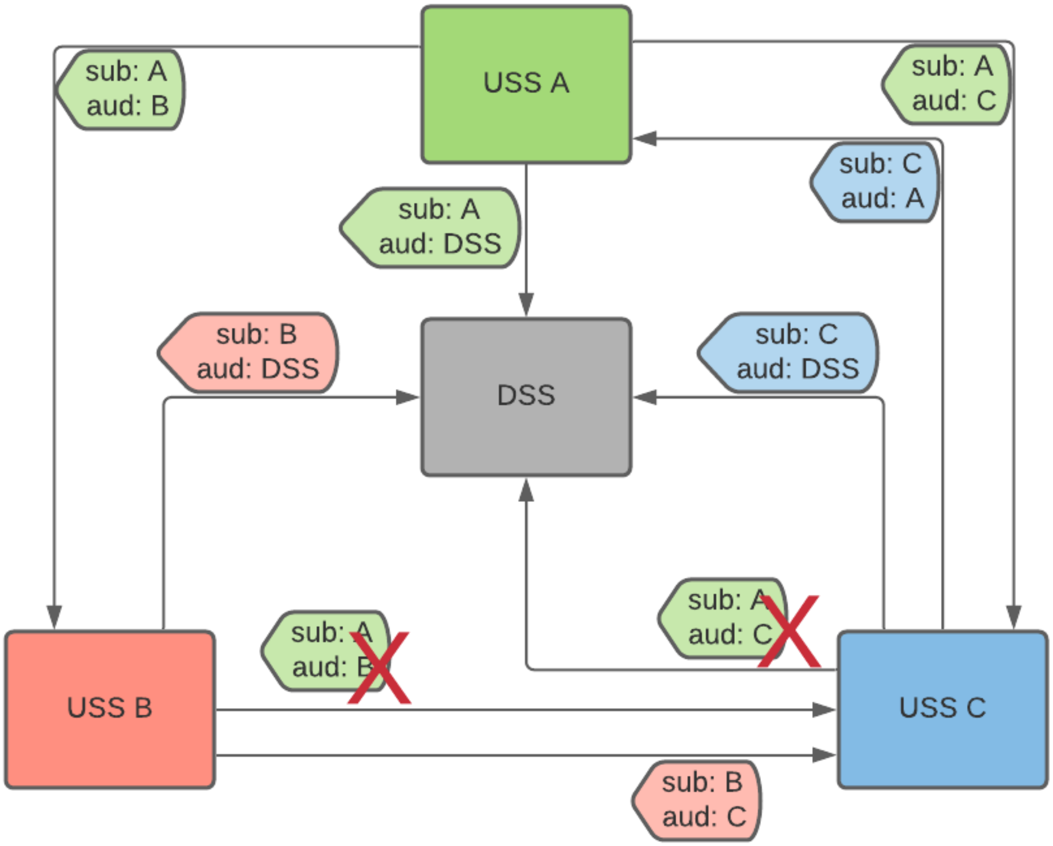


Figure A.1-2. Token Reuse Protection with Audience Claim

In figure A.1-2, light-colored access tokens are used to attempt to access other servers in the federated architecture. USS A is able to correctly contact all other servers. USS B initially attempts to use the access token it received from USS A to access USS C, but the attempt is rejected because USS C does not identify itself with the `aud` claim of “B”, instead expecting “C”. Similarly, USS C initially attempts to use the access token it received from USS A to access the DSS, but this attempt is rejected for a similar reason.

Again here, the audience claim is required at a minimum because it prevents token reuse to access different USSs on all API calls, including ones where message signing (as defined in this project) does not provide any additional security when accessing different USSs. Message signing, as used in the UPP2 project, used JSON Web Signatures (JWS) to sign HTTP calls with bodies. HTTP calls without bodies and replies were not signed, but still protected via the TLS connection.

Short term OAuth outages are supported by design, as per the ASTM Remote ID Standard, tokens are re-requested hourly to enable quick revocation of the user's privileges. Token duration should be set in consideration of reliability (longer durations) versus security risk (shorter durations). In the event of a short-term OAuth outage, existing tokens can continue to be used for a short period of time; thereafter, a fail-safe outcome is achieved by the preclusion of creating new flights with potential conflicts.

A more complete analysis of interoperability failure cases is being performed in support of the draft ASTM UTM USS Interoperability standard, and the standard is being written to ensure a fail-safe outcome in all cases. Our expectation is that failures of OAuth would map to existing interoperability scenarios included in that analysis; however, we recommend the working group validate this assumption.

Both the ASTM Network RID Standard and the ASTM USS Interoperability Standard require a production-like integration environment for ecosystem participants, it would be expected to have the same deployment setup for the integration environment to provide full end-to-end testing. However this may occur with different tokens.

A.2 Enhanced deployed: Access tokens plus message signing

This architecture, which leveraged the ICAO International Aviation Trust Framework (IATF), was used for portions of UPP2 where certificates were obtained and message signing was implemented. As with architecture described in A.1 (access tokens with audience claims), this architecture credibly establishes the identity and authorization scope of the client USS to the server USS as described below. It also enables non-repudiation of some messages: the recipient of a message within the system can prove that a received message with non-empty body originated from someone with access to the private key of the USS indicated as the sender. This architecture accomplishes these goals by cryptographically signing the body content (when it exists) of every message exchanged with another server, in addition to using standard OAuth2 access tokens as described in the previous architecture and transport layer encryption between clients through TLS. There are two possible ways to disseminate the information necessary to validate the message signatures: self-signing or via a certificate authority. In order to maintain non-repudiation and to mitigate impersonation attacks, self signed certificates have to be created, managed and audited ideally using the same processes as a certificate authority (CA) using a trusted Certificate Policy (CP). The USS using self-signed certificates acts as its own CA.

Message signing can provide an additional layer of protection if the TLS layer is compromised or an insider Attack is successfully carried out, hence the internal networks have been breached. This would be considered unlikely with the defined attacker profile which the Working Group has considered

As with the Access Tokens with Audience Claims architecture described above, we expect that message signing failures would also map to existing interoperability scenarios included in the fail-safe analysis being performed for the draft ASTM UTM USS Interoperability standard, which will always result in a fail-safe outcome. We repeat the recommendation that the working group validate that the fail-safe analysis scenarios cover message signing failures.

Message signing could be added to existing deployments incrementally. For example in the FAA UTM Pilot Program 2, there were a mix of providers providing different services. Providers of more safety critical or providing services to government implemented message signing, however the providers of basic and non safety services like Remote ID did not and data exchange was still possible with the non-repudiation benefits for more safety or security critical applications. Separately or in addition, message signing can be used to authenticate a client to the authorization server when requesting an access token.

Trusted Certificate Authority

When a trusted certificate authority is available, that certificate authority can cross-sign CA certificates to endorse each USS's certificate. This architecture variant is illustrated in figure A.2-1.

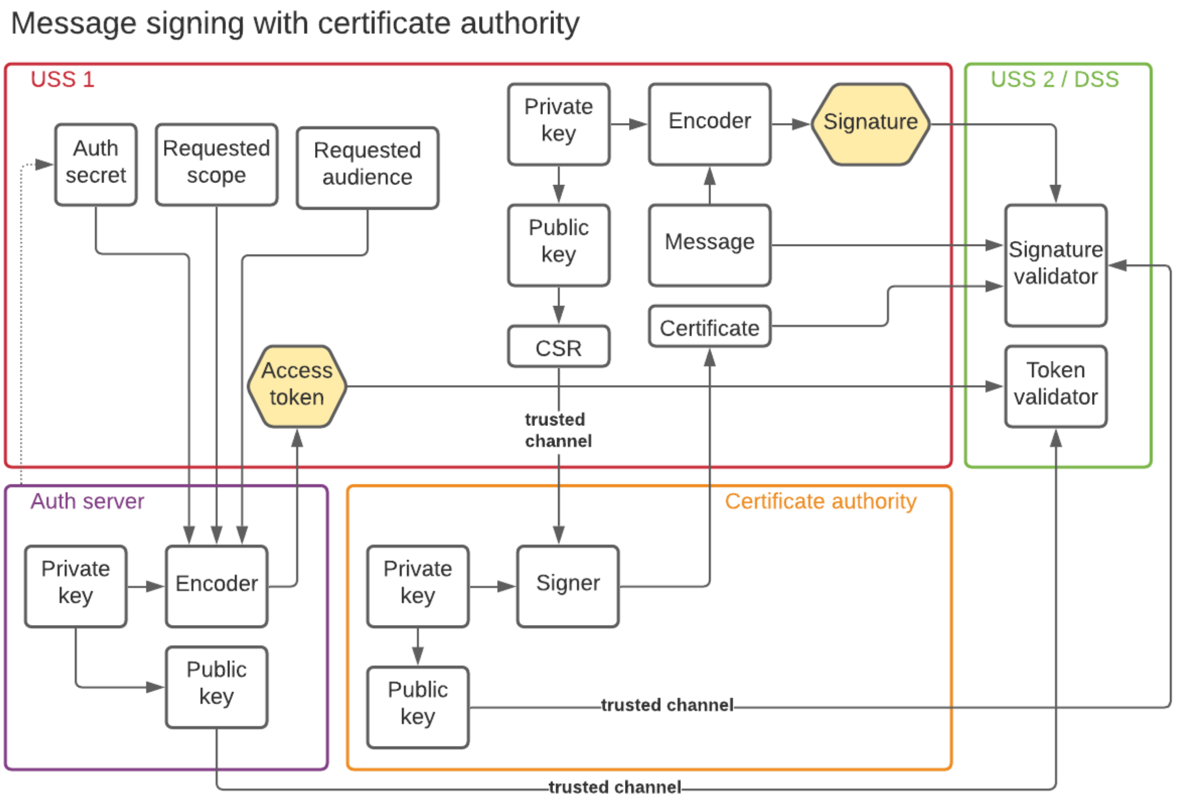


Figure A.2-1. Message Signing with Certificate Authority

Central certificate authorities can be complex and require a rigorous certificate policy framework including strict revocation. In the FAA UTM Pilot Program 2, certificates based on the ICAO Aviation Trust Framework (described further in Appendix B) were used. In the case of a need to revoke access, the first layer would be to revoke the OAuth token--this would still be the initial and fastest form of revocation. The certificate-based revocation process using CRLs would potentially require fast network interaction and extended time to propagate the information about revoked certs through the connected parties. By this the certificate based revocation process would take more time.

Hence the proposed approach is to base the revocation process on removing the OAuth token:

A.3 Self-signed certificates

A central certificate authority may not always exist or may not be immediately available or cost-effective. When a central certificate authority across all parties is not available, and given a small number of UAS Service Suppliers within a region, self-signed certificates from one party local or dedicated Certificate Authority can be utilized. Self-signed certificates would be created as part of the onboarding process of a new USS and the Auth server can take on the additional duty of hosting and distributing each USS’s self-signed certificate. This establishes the Auth server as the authority for which message signing keys were ever used by a USS (for the purposes of non-repudiation), and the trusted source for certificates when validating signatures. This architecture variant is illustrated in the figure below. For some countries, the base deployment with access tokens with audience claims is initially sufficient for providing safety benefits and may be preferred over self-signed certificate management. In order to maintain non-repudiation and to mitigate impersonation attacks, self signed certificates have to be created, managed and audited ideally using the same processes as a certificate authority (CA) using a trusted Certificate Policy (CP). The USS using self-signed certificates acts as its own CA.

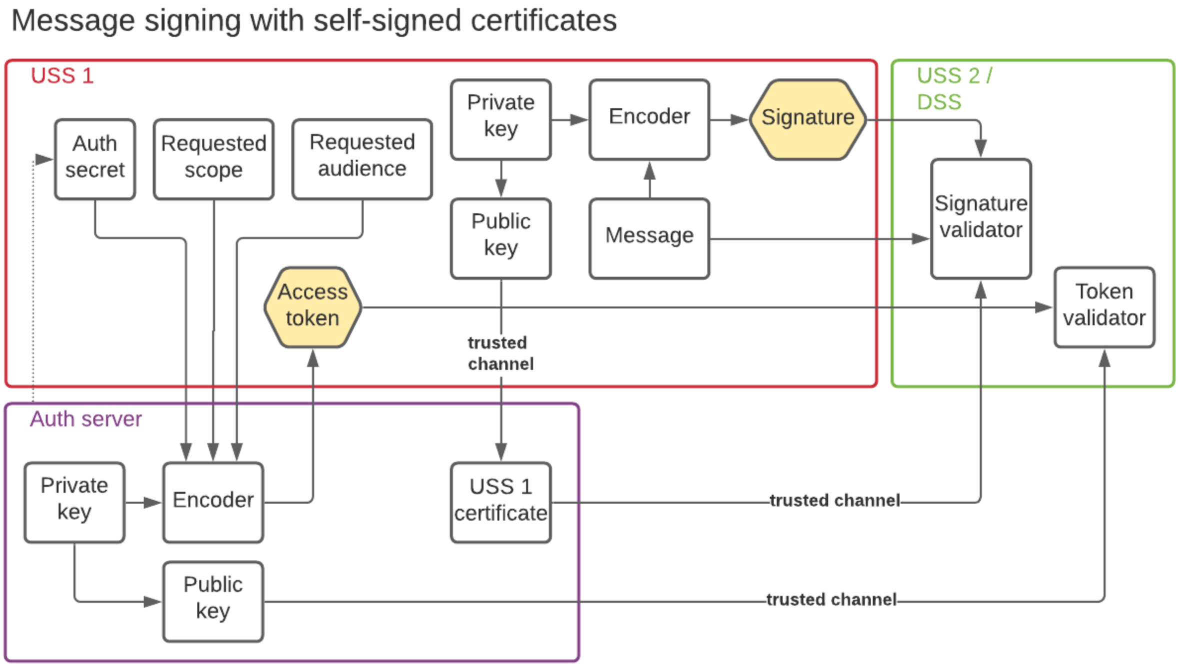


Figure A.3-1. Message Signing with Self-Signed Certificates

Appendix B - International Civil Aviation Organization (ICAO) Aviation Trust Framework (IATF)

The IATF is in a formative stage. The impetus for the IATF is that the cost of aviation-specific communications infrastructure is becoming prohibitive. It is therefore desirable to be able to use internet protocol based secure overlay communication over public communications infrastructure (e.g., the internet and commercial IP based network providers) to support aviation-specific communications; however, this requires a sufficient security framework to ensure the safety of the global aviation system (i.e., the large collection of systems -- ANSP-provided ATC systems, voice communications, navigation, surveillance, airport systems, airline systems, and many others -- that provide aviation services across the globe, as illustrated in Figure B.1).

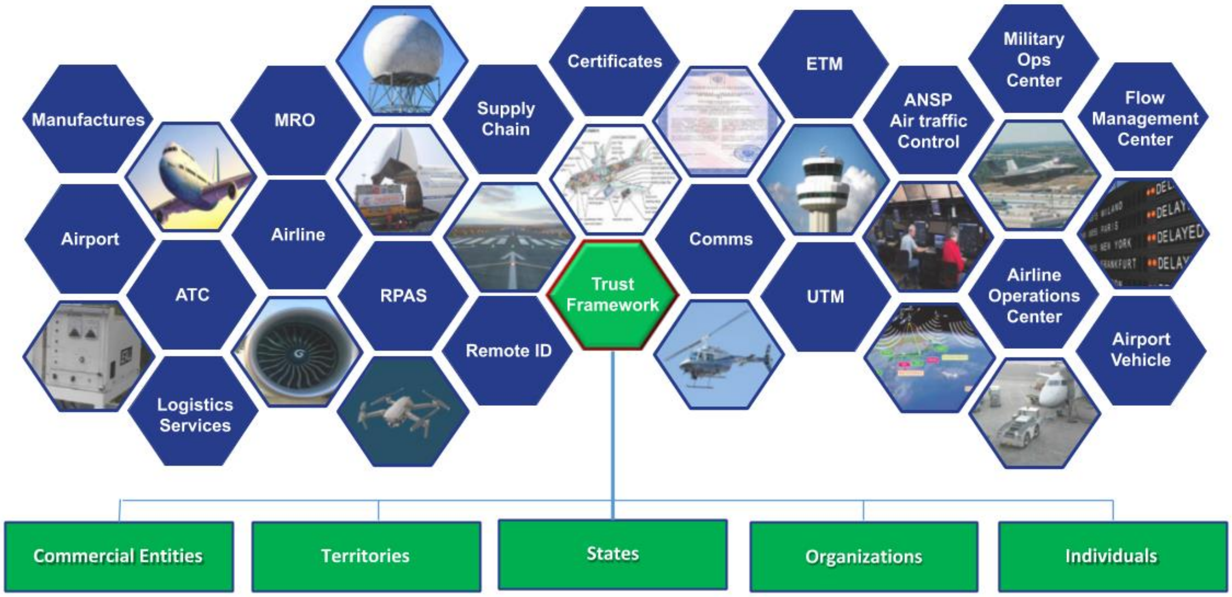


Figure B.1. Scope of Global Aviation System

Key overall objectives of the IATF include:

1. That IATF participant identities are trustable, achieved through:
    a. A common IATF master trust framework agreement, and
    b. Common identity policies audited through the IATF
2. That information flow between IATF participants are attributable to the IATF identity source of the information by digitally signing the information
3. That IATF-compliant networks, called Global Resilient Aviation Information Networks (GRAINs), are trustable, through:
    a. Trusted network addressing,
    b. Trusted domain naming services, and
    c. Trusted network operations through IATF-audited Information Security Management System (ISO 27000/NIST).

The proposed IATF organizational structure is shown in Figure B.2. Underneath the board and advisory components shown at the top, the core of the organization is two main parts guided by a program management office. The first part focuses on policy; the second part on operational services provided in accordance with the established policy.

Within the policy group, there are two focus areas: identity policy services, which addresses policy associated with Certificate Authorities (CAs); and, network policy services, which addresses other policies associated with participation in the aviation network.

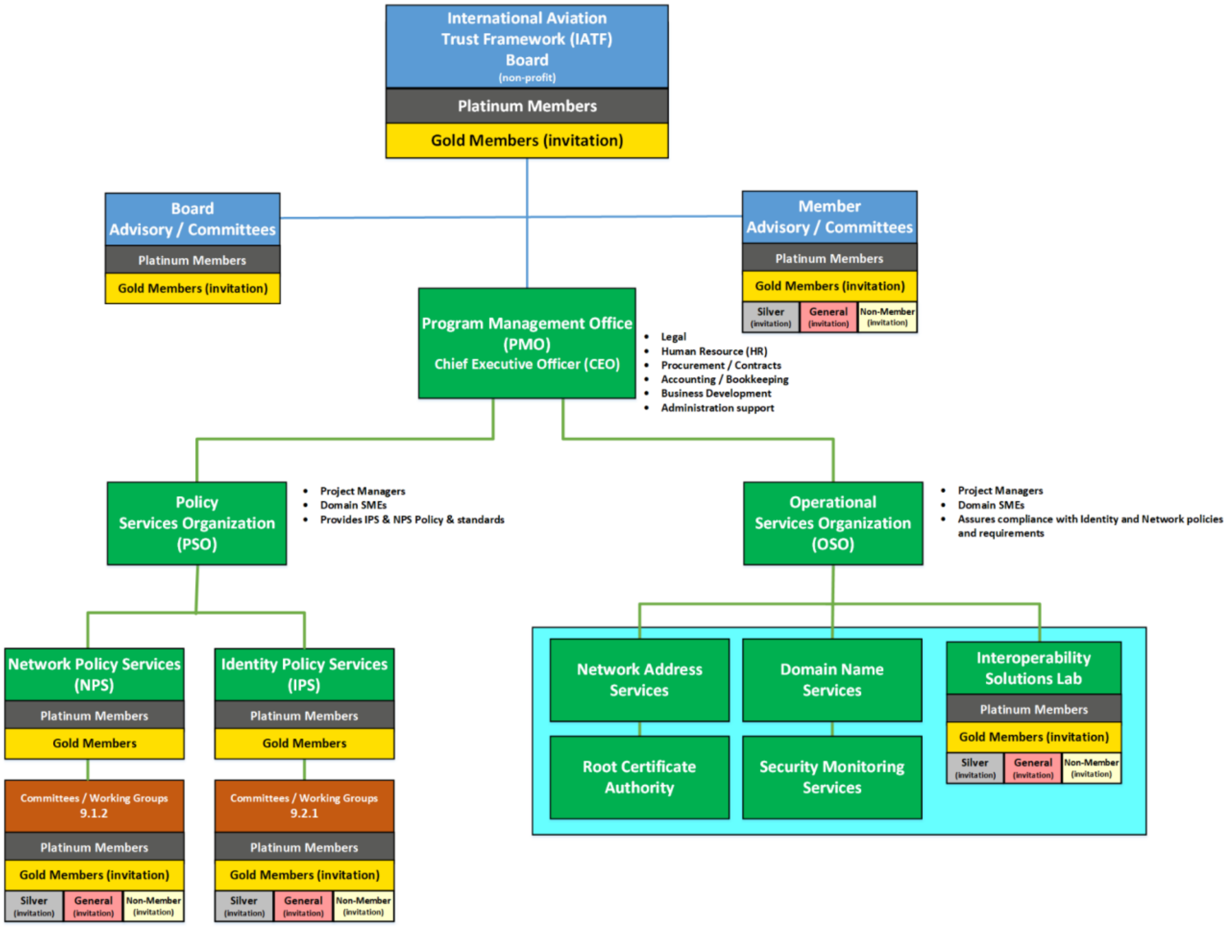
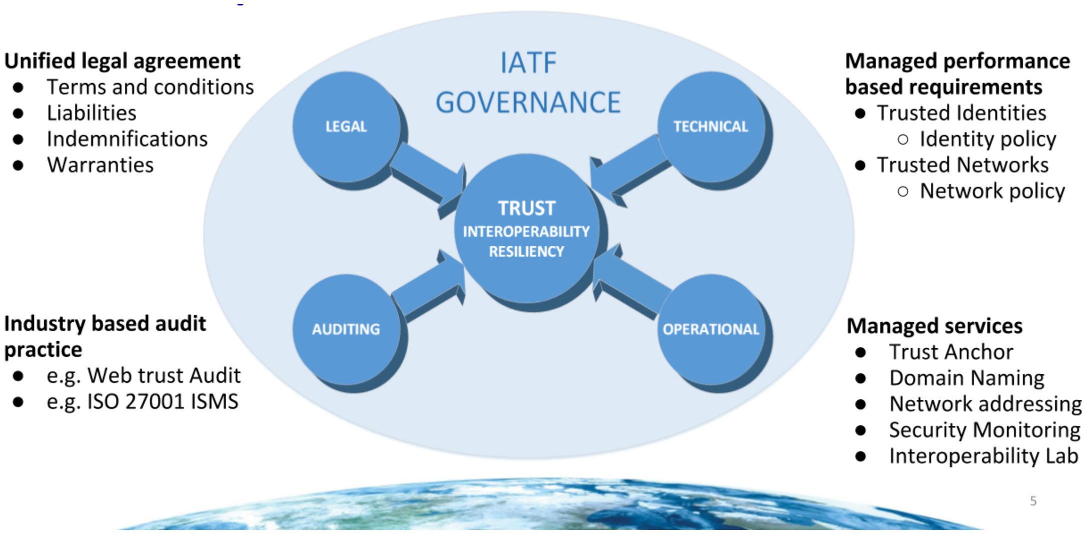

International Aviation Trust Framework (IATF) Board (non-profit)
Platinum Members
Gold Members (invitation)
Board Advisory / Committees
Platinum Members
Gold Members (invitation)
Member Advisory / Committees
Platinum Members
Gold Members (invitation)
Silver (invitation)
General (invitation)
Non-Member (invitation)
Program Management Office (PMO)
Chief Executive Officer (CEO)
Legal
Human Resource (HR)
Procurement / Contracts
Accounting / Bookkeeping
Business Development
Administration support
Policy Services Organization (PSO)
Project Managers
Domain SMEs
Provides IPS & NPS Policy & standards
Operational Services Organization (OSO)
Project Managers
Domain SMEs
Assures compliance with Identity and Network policies and requirements
Network Policy Services (NPS)
Platinum Members
Gold Members
Committees / Working Groups 9.1.2
Platinum Members
Gold Members (invitation)
Silver (invitation)
General (invitation)
Non-Member (invitation)
Identity Policy Services (IPS)
Platinum Members
Gold Members
Committees / Working Groups 9.2.1
Platinum Members
Gold Members (invitation)
Silver (invitation)
General (invitation)
Non-Member (invitation)
Network Address Services
Domain Name Services
Root Certificate Authority
Security Monitoring Services
Interoperability Solutions Lab
Platinum Members
Gold Members (invitation)
Silver (invitation)
General (invitation)
Non-Member (invitation)

Figure B.2. Proposed IATF Organization Structure

A variety of membership levels are available. Consideration has been given to ensure commercial service providers cannot unduly influence policy (e.g., to require the use of a particular proprietary solution).

The scope of the IATF is shown in Figure B.3. In addition to establishing identity and network policy, and overseeing the provision of compliant operational services, the IATF would also produce unified legal agreements pertaining to the provision and use of the services and an industry-based audit practice.



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

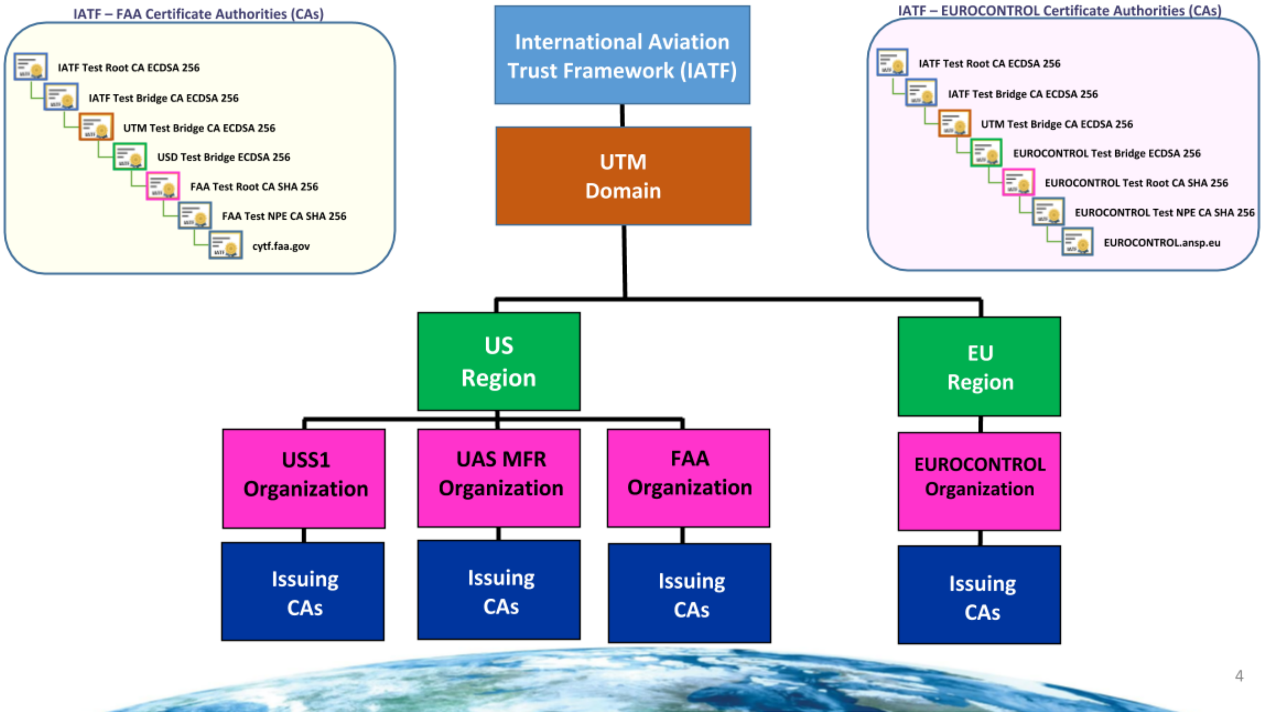
Managed performance based requirements
- Trusted Identities
  - Identity policy
- Trusted Networks
  - Network policy

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

Figure B.3. IATF Scope

The IATF governance model is illustrated in Figure B.4. In the case of the UTM domain, multiple regions (US, EU, etc.) would be established allowing service providers to be region-specific, but still falling under the overall policies of the IATF.



IATF – FAA Certificate Authorities (CAs)

- IATF Test Root CA ECDSA 256
  - IATF Test Bridge CA ECDSA 256
    - UTM Test Bridge CA ECDSA 256
      - USD Test Bridge ECDSA 256
        - FAA Test Root CA SHA 256
          - FAA Test NPE CA SHA 256
            - cytf.faa.gov

IATF – EUROCONTROL Certificate Authorities (CAs)

- IATF Test Root CA ECDSA 256
  - IATF Test Bridge CA ECDSA 256
    - UTM Test Bridge CA ECDSA 256
      - EUROCONTROL Test Bridge ECDSA 256
        - EUROCONTROL Test Root CA SHA 256
          - EUROCONTROL Test NPE CA SHA 256
            - EUROCONTROL.ansp.eu

Figure B.4 IATF Governance Model