UTM Key Site Operational Evaluation

Industry Operator Consortium Meeting

UTM
UAS TRAFFIC MANAGEMENT

December 2023

Note: this presentation was delivered in December 2023 and some content may no longer be current.

Federal Aviation Administration

UTM Implementation Security Considerations

UTM Information Security Overview

Information exchange is central to enable UTM interoperability between partners and users. With exchanges occurring across public internet, UTM information should be protected according to federal guidelines.

NIST Special Publication 800-12 defines the Confidentiality, Integrity, and Availability Triad (CIA Triad) as the three pillars of information security:

- ***Confidentiality**, **integrity**, and **availability** are key to ensuring that UTM systems prioritize the protection and accuracy of data and maintain uninterrupted services*

UTM consists of several types of interfaces, each which require appropriate interoperable security controls to ensure the information security of the overarching UTM ecosystem:

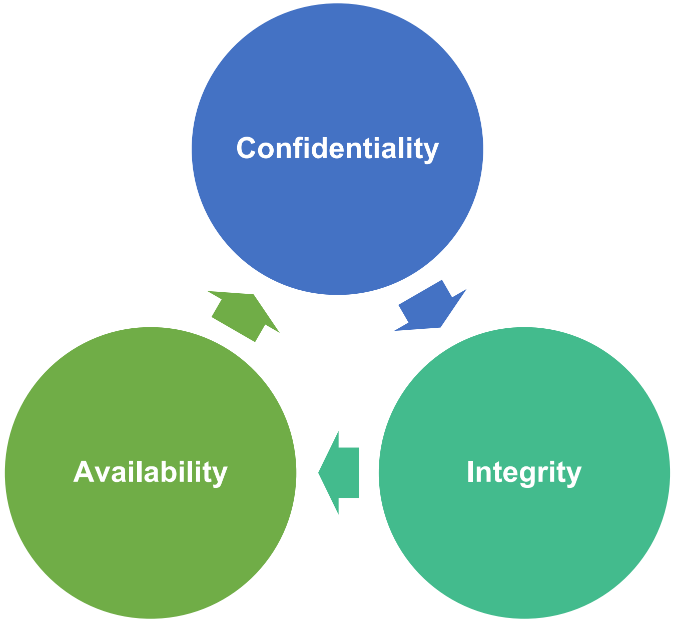
System-to-System Interfaces

- USS-USS Exchanges: Communication for strategic deconfliction
- USS-SDSP Exchanges: Weather, surveillance, performance

User-to-System Interfaces

- USS-Operator: Real-time information, operational intent
- System Administrator: System configuration

NIST CIA Triad



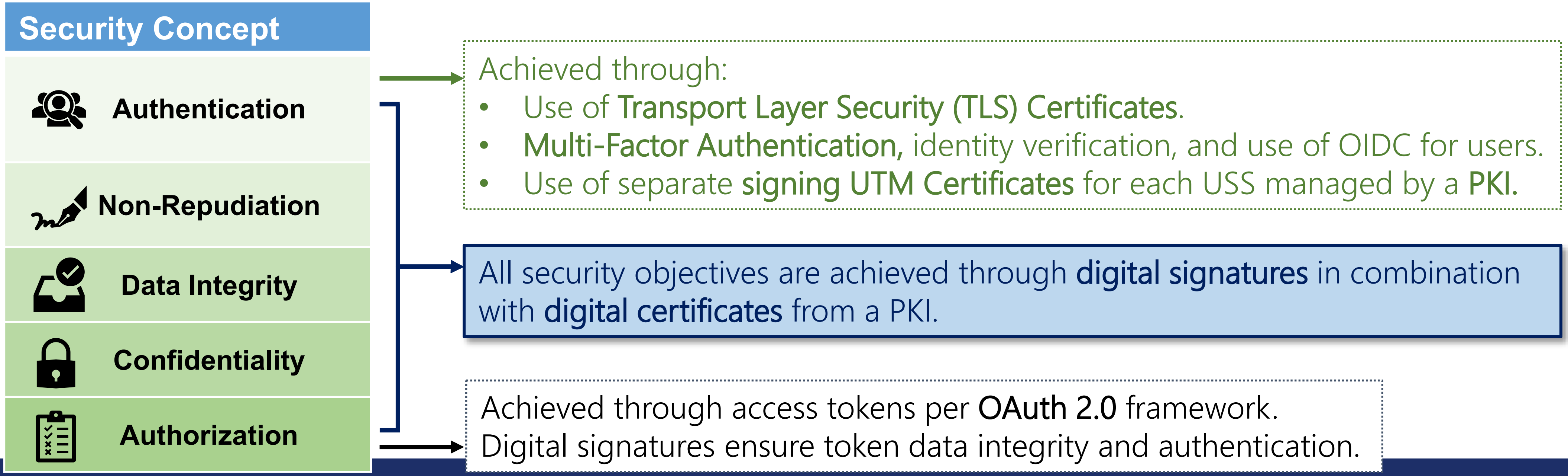
Need for Information Security in UTM

- Communications between UTM entities and users (e.g., for situational awareness, deconfliction) must be adequately secured to ensure interoperability of operations and integrity of messages exchanges:
  - If UTM information is altered intentionally or unintentionally, strategic deconfliction may fail, increasing the risk to potential incidents
  - Bad actors may be able to spoof a USS or cause a denial-of-service attack
  - Discrepancies between data can cause loss of trust in the UTM ecosystem

Security Concept	Information Security Need
Authentication	• UTM information exchanges over public internet leave UTM participants vulnerable to intercepted messages. • Verify the identity of the message sender to ensure a trusted data exchange. • Username/password credentials likely do not provide adequate level of security.
Non-Repudiation	• An incident may occur where there are discrepancies between data of two USS. • Non-repudiation provides proof of message sender's identity and confirmation the message came from the sender, cannot refute messages later in instance of USS-USS conflict. • Logging each message sent can be costly and logs can be susceptible to tampering.
Data Integrity	• Altered UTM data can cause corrupt data such as operational plans and constraints sent to stakeholders. • Corrupted messages can cause strategic deconfliction to fail or off-nominal messages to be generated erroneously.
Confidentiality	• Operational plans may contain sensitive or proprietary data. • Protect sensitive operations information (e.g., certain operations) from unauthorized parties' interception.
Authorization	• UTM services should only be provided by parties qualified to provide service. • Requests for sensitive or proprietary data should only be provided to those authorized to participate in the system. • Access token requests should be from a credentialed source and tokens received should not been tampered with.

Message Signing Approach for UTM

- Consistent user security approaches allow a secure and consistent user experience for UAS operators and system administrators.
- Combination of Public Key Infrastructure (PKI) with digital signature increases trust across organizations
- JSON Web Signature (JWS) has been validated in multiple demonstrations to be:
  - Compatible with ASTM USS-USS Interoperability Standard, JSON messages
  - Relatively easy to implement after system updates are applied
  - Single step that does not require additional logs, hash
  - Encryption can be added with a similar approach using JSON Web Encryption (JWE)



Security Concept

- **Authentication**
- **Non-Repudiation**
- **Data Integrity**
- **Confidentiality**
- **Authorization**

Achieved through:

- Use of **Transport Layer Security (TLS) Certificates**.
- **Multi-Factor Authentication,** identity verification, and use of OIDC for users.
- Use of separate **signing UTM Certificates** for each USS managed by a **PKI.**

All security objectives are achieved through **digital signatures** in combination with **digital certificates** from a PKI.

Achieved through access tokens per **OAuth 2.0** framework. Digital signatures ensure token data integrity and authentication.

Implementation of Authorization Server

- Use of OAuth 2.0 Framework for USS-USS, USS-FIMS, and USS-DSS message exchange authorization
  - Authentication to authorization server for access token request:
    - Strong authentication (e.g., digital signature) in alignment with the UTM Implementation Plan to ensure non-repudiation
- Requirements need to be ensured for:
  - Auditing of authorization server to allow FAA oversight
  - Processes to revoke USS both by authorization server host and by FAA
- Consider integrating the authorization server with the test harness to translate service approval results into permissions

Backup Information

Information Security Objectives in UTM

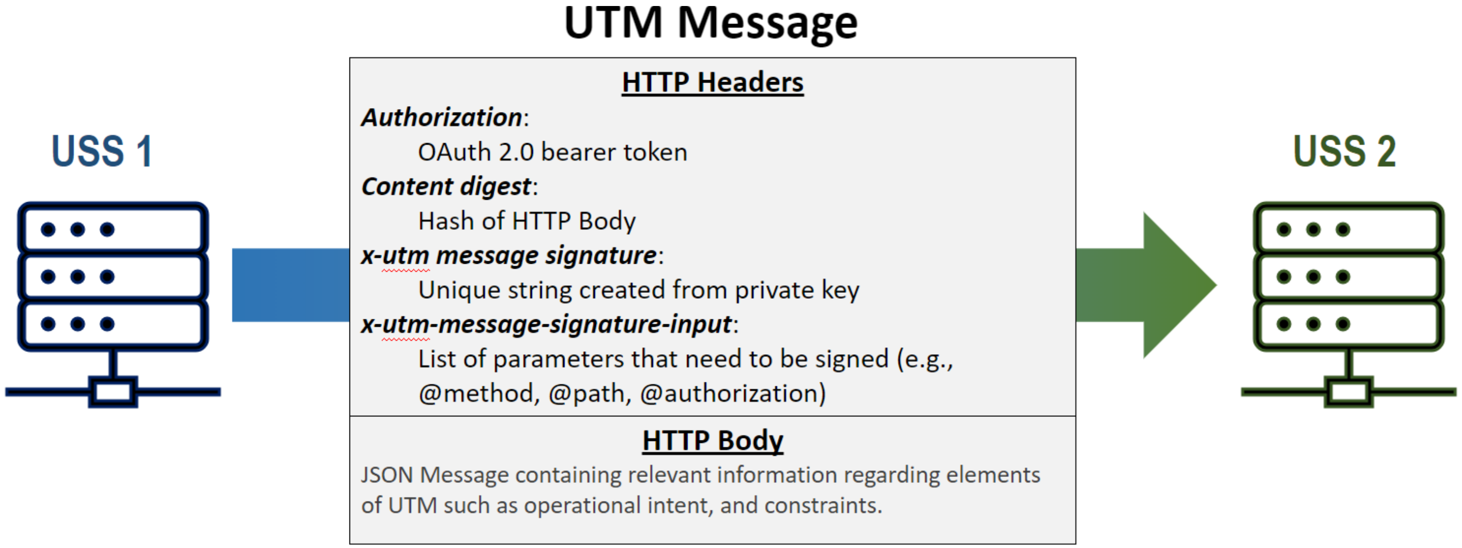
- Communications between UTM entities and users (e.g., for situational awareness, deconfliction) must be adequately secured to ensure interoperability of operations and integrity of messages exchanges
- UTM can leverage security standards from NIST and ASTM USS-USS Interoperability to maintain a harmonized security approach all information exchanges
- Consistent user security approaches allow a secure and consistent user experience for ***UAS operators*** and ***system administrators***

Security Concept	Definition
Authentication	Identity verification of the message sender through credentials (e.g., username/password, digital certificate, multi-factor authentication)
Non-Repudiation	Proof that the sender sent a message
Data Integrity	Protection from intentional or unintentional modification
Confidentiality	Message contents concealed from unauthorized service providers
Authorization	Access limited to appropriately permissioned service providers

Message Signing Approach for UTM Ecosystem

- FAA, NASA, and industry developed an initial set of signing requirements* in previous UTM activities
  - Used IETF draft RFC** as standard approach for signing HTTP messages in UTM
  - Digital certificates were sourced to the prototype CA from the FAA
  - Based on success of message signing testing, use of message signing for UTM implementation should be achievable

- Implementation recommendations include:
  - Updating DSS to require signed messages and DSS signature validation
  - Determining requirements for digital certificates used for message signatures



UTM Message

HTTP Headers

Authorization:
OAuth 2.0 bearer token

Content digest:
Hash of HTTP Body

x-utm message signature:
Unique string created from private key

x-utm-message-signature-input:
List of parameters that need to be signed (e.g., @method, @path, @authorization)

HTTP Body

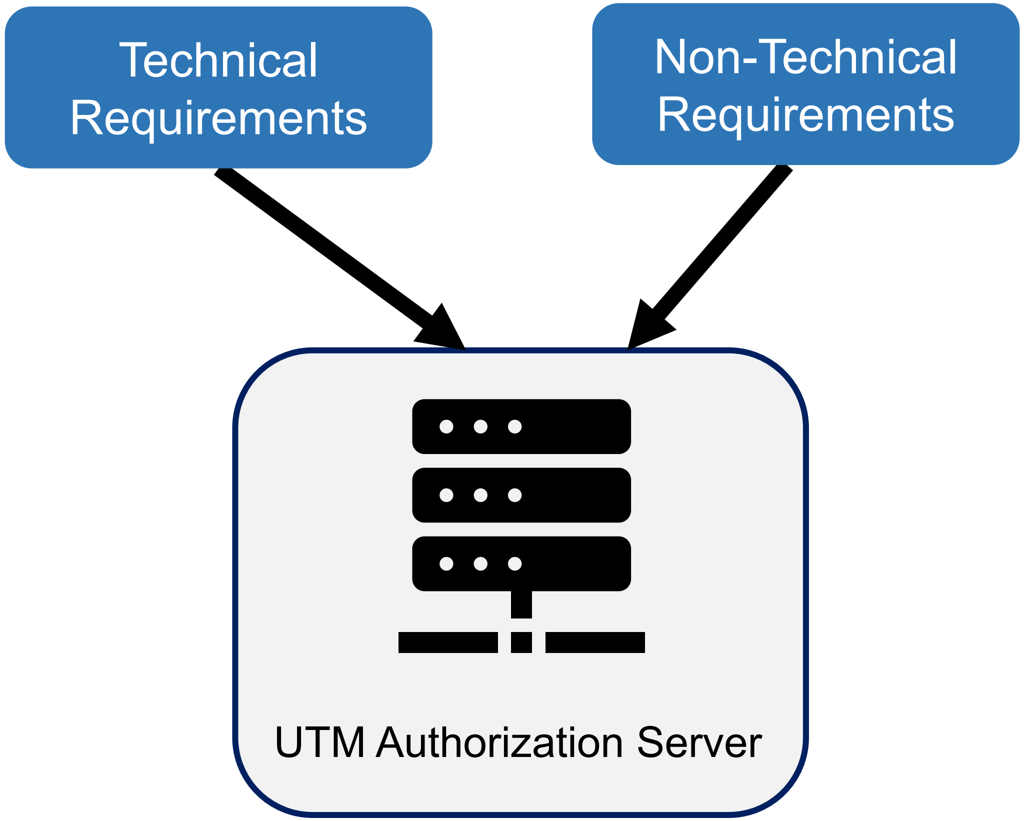
JSON Message containing relevant information regarding elements of UTM such as operational intent, and constraints.

* NASA. "*Non-Repudiation for Drone-Related Data.*" TM-20220016658 (2022)

**https://httpwg.org/http-extensions/draft-ietf-httpbis-message-signatures.html

Considerations for UTM Authorization

- A number of aspects of the authorization server must be determined for UTM implementation
  - *Technical requirements*: authentication mechanism, specific OAuth grants, token validity time, server availability, etc...
  - *Non-technical requirements*: governance, onboarding, offboarding, management of scopes, revocation of access, FAA access
- Industry must come to consensus on these elements to ensure that the authorization server meets the needs across industry entities
  - With industry consensus, industry can bring approach to the FAA who can then concur on the agreed-upon approach
  - Since the UTM ecosystem has a federated nature, agreement on authorization helps build trust between participating suppliers


Technical Requirements
Non-Technical Requirements
UTM Authorization Server