USS Specification

Introduction

Within the Unmanned Aircraft Systems (UAS) Traffic Management (UTM) system, the UAS Service Supplier (USS) is a key component. The USS serves several functions. At a high level, those include the following:

- Bridging communication between UAS Operators and Flight Information Management System (FIMS)
- Supporting planning of UAS operations
- Assisting strategic deconfliction of the UTM airspace
- Providing information support to UAS Operators during operations
- Helping UAS Operators meet their formal requirements

This document provides the minimum set of requirements for a USS. In order to be recognized as a USS within UTM, successful demonstration of satisfying the requirements described herein will be a prerequisite.

To ensure various desired qualities (security, fairness, availability, efficiency, maintainability, etc.), this specification relies on references to existing public specifications whenever possible. References are indicated using square brackets.

Notational Conventions

The key words 'MUST,' 'MUST NOT,' 'REQUIRED,' 'SHALL,' 'SHALL NOT,' 'SHOULD,' 'SHOULD NOT,' 'RECOMMENDED,' 'NOT RECOMMENDED,' 'MAY,' and 'OPTIONAL' in this document are to be interpreted as described in [RFC2119].

The key word definitions form a well-defined superset of the NASA recommended language for requirement description found in [NASASysEng].

Requirements (i.e., "MUST" statements) are indicated in green, italicized sentences, with each sentence being a single requirement.

Terminology

A USS is discussed with an active voice, as if it is an organization or entity, when in reality it is a collection of software. When a statement such as "A USS may do this" is made it is understood to mean that "A software implementation adhering to the USS Specification may be implemented to do this". This is a stylistic choice for the goal of clarity, which may or may not be achieved.

For lack of other current terminology, all operations that are not either compliant with Part 107 (i.e., commercial operations) or Part 101, Subpart E (i.e., hobbyist operations) will be called "Part 107X operations" until there is a more appropriate term or rule introduced. Also, in this document Part 101, Subpart E will be abbreviated as "Part 101E."

This document defers other UTM definitions to the [UTMGlossary]. No other new terminology is introduced in this document.

USS Overview

The overall description of a USS within UTM is provided in [UTMConOps]. If there exist discrepancies between that document and this one, deference is to this document since it is more current. To ground discussion regarding the various components int he UTM System and illustrate the position of USSs within it, Figure 1 is provided (in updated form) from the [UTMConOps]:

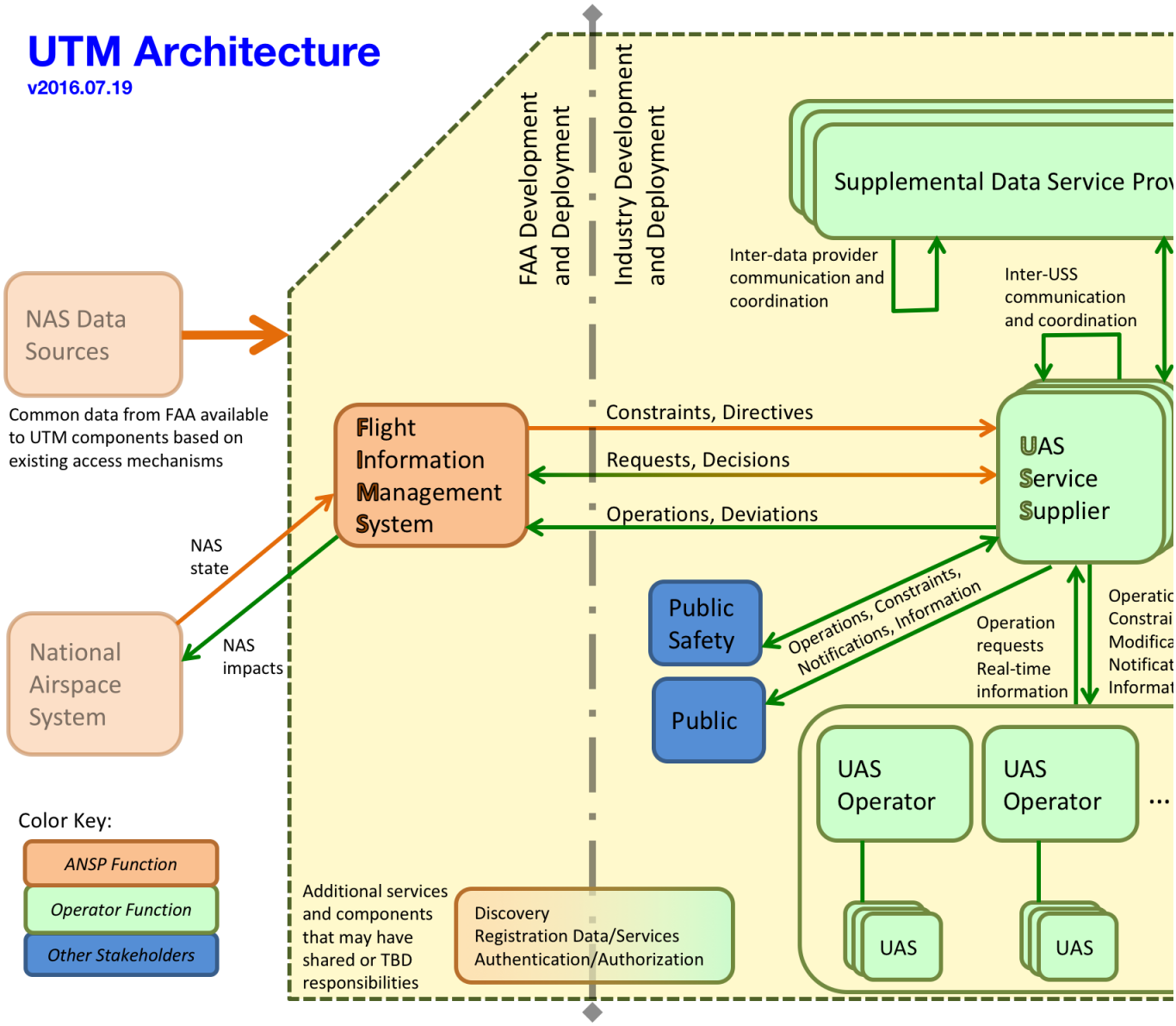

Figure 1. UTM Architecture.

In order to avoid unintended discrepancies, no further summary or details are provided on the USS role or concept within UTM. Rather the details and requirements for implementing a USS are provided herein.

Application Programming Interfaces

Data exchange and, by extension, overall operation of the UTM System is governed by a set of published Application Programming Interfaces (APIs). These APIs are the normative documents for formatting data, defining Internet endpoints, and specifying transfer protocols. This document serves to define requirements not easily captured in the APIs. Whenever possible, this specification defers to the most current applicable API. If there is a discrepancy between this specification and an API specification, the API specification will be given preference. Any discrepancies should be reported to the author of this document as soon as possible to allow for timely correction (either in this document or within an API).

The API documentation is provided in a format (OpenAPI Specification) such that code may be generated from the API.

The following is a brief overview of the APIs relevant to the USS Network (see [UTMGlossary] for a formal definition of "USS Network").

FIMS-USS API

The [FIMSUSS-API] is the most central API in that it defines all data exchanges between FIMS and any USS. The definitions within [FIMSUSS-API] describe the submission of operation plans, messages, and positions to FIMS from a USS. It also defines various subscription endpoints wherein a USS will receive asynchronous updates to the UTM airspace and UTM operation data.

USS-USS API

The [USSREQ-API] defines the required interfaces that each USS (or USS Instance) must support to allow interoperability within the USS Network and focuses on data exchange between USSs. See [UTMGlossary] for a formal definition of a USS Instance.

USS Discovery Service API

The [USSDS-API] defines the interface to the FIMS-provided USS Discovery Service (USSDS). This discovery service allows for USSs and UAS Operators to be aware of USS Instances providing USS services of potentially varying levels of capability to specific geographical regions. USSs are required to interact with the USS Discovery Service to establish resolvable named endpoints and the scope of the services that the USS Instance will provide.

FIMS Authorization API

The [FIMSAuthzAPI] provides the interface definition to authorization services for FIMS and USSs within the UTM System. This is an OAuth 2.0-based system. The UTM-specific design choices within the OAuth 2.0 framework are described partly within this specification and more completely in the [FIMSAuthzAPI] documentation. The latter is considered the official source in the case of any discrepancies in documentation.

UTM Keys

Overall, the management of cryptographic keys within the UTM System will be guided by the three National Institute of Standards and Technology (NIST) documents in the "Recommendation for Key Management" series: [NIST.800.57.p1] (general), [NIST.800.57.p2] (best practices), [NIST.800.57.p3] (application-specific). Based on further review of those documents, this section will become more formalized and specific.

UTM-USS-001
As part of the checkout process, the applying organization MUST generate a public-private key pair (UTM-PUBLIC-KEY and UTM-PRIVATE-KEY) using the RSA approach [RFC8017][RSA].

UTM-USS-002
The applying organization MUST supply the generated UTM-PUBLIC-KEY to the UTM regulator.

As part of the checkout process, the applying organization MUST generate a public-private key pair (UTM-PUBLIC-KEY and UTM-PRIVATE-KEY) using the RSA approach [RFC8017][RSA]. The applying organization MUST supply the generated UTM-PUBLIC-KEY to the UTM regulator. Upon completing this requirement, the UTM-designated certificate authority (CA) will generate a public certificate (UTM-ISSUED-CERT) and supply that to the organization. This public certificate will be available to other stakeholders within UTM. This public certificate will serve as part of the authentication process for certain data transactions within UTM as specified in this document.

The organization MUST obtain a public certificate (INTERNET-PUB-CERT) from a certificate authority within the Common CA Database [CCADB] that has a geographic focus that includes "USA." This public certificate will be used for certain connections to and from other UTM components as specified in this document.

Random Numbers

Random numbers are a part of other requirements described in this document. [NIST800.90A.R1] describes methods of generating Deterministic Random Bit Generation (DRBG) and [NIST800.90A.R1.LIST] provides a list of validated implementations adhering to those methods. *When generating a random number for any purpose within the UTM System, a USS MUST use a method adhering to the recommendations in [NIST800.90A.R1].*

UUID Generation

The generation of Universally Unique Identifiers (UUIDs) are a necessary part of a USS operation. *When generating a UUID, a USS MUST generate a version 4 UUID as per [RFC4122].* A parallel reference for UUID generation by the International Telecommunication Union [ITUX.677] is also available and likely compatible with the referenced RFC, but this specification defaults to [RFC4122] for clarity.

JSON Data

Data exchanges with the UTM System are primarily accomplished via JavaScript Object Notation (JSON)-defined data schemas. The specific schemas will be provided to stakeholders as [OpenAPIv2] specifications whenever possible. The [OpenAPIv2] specification references the [JSONSpec], but may redefine or add certain terms. As such, when schemas are described using [OpenAPIv2], that specification will be the defining reference. At times where JSON is used outside of an [OpenAPIv2] description, the [JSONSpec] will be the defining reference.

For any exchange of JSON-formatted data, the receiver MAY ignore any fields that are supplied by the sender that are not included in the relevant schema definition.

For any exchange of JSON-formatted data, the receiver MUST ignore the entirety of the received data whenever any required field (as specified in the relevant schema definition) of the received data is missing or malformed. If missing/malformed data are received via a RESTful call, the receiver MUST reply with an HTTP 400 status code.

USS Authorization

The USS Network relies on the OAuth 2.0 Framework as described in [RFC6749] for authorizations. *A USS MUST obtain an access token from the FIMS Authorization Server using the published [FIMSAuthzAPI]. Authentication of the USS with the FIMS Authorization Server MUST be completed via Transport Layer Security (TLS) 1.2 client authentication using the USS INTERNET-PUB-CERT*. Proper implementation of TLS 1.2, including the protocol for requesting certificates from a client, is defined in [RFC5246]. The assumption regarding access key usage and management is that a USS will share the current access token for a given set of scopes within its set of USS Instances as needed. The scopes are defined in the [FIMSAuthzAPI]. The provided token is a bearer token as defined in [RFC6750]. The terms "access token" and "bearer token" will be used interchangeably in this document, with the chosen term based on context and in reference to other documents.

The bearer token provided to a USS by the FIMS Authorization Server will be a Java Web Token (JWT) as defined in [RFC7519]. *A USS MUST be able to decode a properly formatted JWT.* The bearer token will be signed as a Java Web Signature (JWS) as defined in [RFC7515]. *The USS MUST be able to check a JWS for validity*.

The above text is considered normative for this specification and the following diagram is informative of those concepts:

Figure 2. USS Request of Access Token.

To ensure continuity of service for a USS and its Instances, the USS SHOULD request new access tokens sufficiently prior to the expiration of existing tokens when needed.

Access tokens are required for authorization on various endpoints in the referenced UTM APIs. *A USS MUST NOT accept a JWT when the current time is greater than the "exp" claim value in the JWT. A USS MUST NOT accept a JWT when the current time is earlier than the "nbf" claim value of the JWT. A USS MUST NOT accept a JWT wherein the "iss" claim does not match the URL of the FIMS Authorization Server. A USS MUST NOT accept a JWT wherein the scope is insufficient for the resource being requested. A USS MUST NOT accept a JWT wherein the "sub" claim cannot be mapped to the data provided on a submission.* This requirement is appropriate, for example, when a USS POSTs operation data to another USS. If the JWT does not match the noted USS within the operation plan, the plan is disregarded.

A USS MUST exclusively support token exchange via the Authorization Request Header Field as per [RFC6750] Section 2.1. A USS MUST respond to a request requiring an access token that is missing an access token according to [RFC6750] Section 3.

If introspection is allowed by the FIMS Authorization Server, the API will be described in the [FIMSAuthzAPI]. A USS MAY use the introspection endpoint for token introspection as per [RFC7662].

If multiple requests for an access token with the same scopes are received from a single USS while a valid access token for that identity-scopes pairing already exists, the same token may be returned to the USS on each of those requests. The FIMS Authorization Server will issue a new access token if there is no currently valid token with at least 5 minutes of time available until its "exp" claim value.

USS Instances

A USS MAY register a USS Instance at any time the USS Discovery Service as hosted by FIMS is operational. This process involves the sending of data to the USSDS describing the USS Instance. *When registering a USS Instance, the USS MUST adhere to the current [USSDS-API]*. A registration that does not include active and responsive endpoint definitions may be rejected by the USSDS. For example, if the callback address for receiving USSDS data is not responsive, the initial registration will fail. A USS Instance may be removed from the USSDS and/or operational data submitted by that removed USS Instance may be rejected if the USS Instance fails to adhere to this specification. In order to ensure a

minimal level of stability in the USS Network, there needs to be an understanding of how long-lived a USS Instance will be. *A USS Instance MUST have a total active time (time_available_end - time_available_begin) of at least one hour*. A USS may remove a USS Instance from active status via an appropriate call to the USSDS.

New USS Instances

USS Instance A will receive notifications about a new USS Instance B (from a different USS) via an endpoint specified by [USSREQ-API] and provided by the USS when registering USS Instance A. *When a USS Instance is notified of another USS Instance being established, the first USS Instance MUST check if the second USS Instance intersects in time and space with the first USS Instance. If a new USS Instance intersects an existing USS Instance maanged by a different USS, both of those USS Instances MUST accept appropriate data requests from the other according to the [USSREQ-API]*. If a USS manages two USS Instances that intersect, the communication between those Instances may be handled internal to the USS.

An illustration of these steps is provided in the following sequence diagrams:

Figure 3. USS Discovery Registration.

Figure 4. USS Registration with Notification.

For details on the HTTP endpoints and data schema, the normative reference is [USSDS-API].

The set of USS Instances with which a particular USS Instance intersects is that USS Instance's "Local USS Network" or LUN. Since the definition of a USS Instance's LUN depends on its intersections, each LUN will likely be different for each USS Instance. For illustrative purposes, the following figure is provided:

Figure 5. USS Instance Intersections

Assume each of the polygons is the operational area covered by a USS Instance. Assume each color represents a different USS, so one USS manages A1 and A2 while another USS manages D1 and D2. The LUN for B is A1, C, and E. The LUN for C is just B. The LUN for A1 is A2 and B, however, the required interfaces between A1 and A2 are relaxed since they belong to the same USS. The assumption in this case is that the USS managing those two USS Instances handles necessary coordination communication. This may be through the established USS APIs or some other method. The LUN for D1 is empty, as is the LUN for D2.

Units of Measure

A USS MUST adhere to API specifications related to units of measure and their formatting. These units will include measurements for speed, distance, altitude, weight, time and other elements. In many cases, metadata related to precision will be specified in the API documentation as well. Details on particular units are intentionally unavailable in this document in order to defer to the authoritative API documentation. Any discrepancy between this document and API documentation defers to the latter.

Date-Time Format

All date-time values exchanged within the USS Network will use [ISO8601] for formatting guidance. *All date-times supplied by a USS between FIMS or another USS MUST follow the format pattern YYYY-MM-DDThh:mm:ss.sssZ. A USS MUST correctly parse time strings with the format pattern YYYY-MM-DDThh:mm:ss.sssZ. A USS MUST persist all date-times following the format pattern YYYY-MM-DDThh:mm:ss.sssZ.* This implies the use of UTC time (denoted with the "Z") for all time stamps. According to [ISO8601], the three fractional decimal places for seconds corresponds to millilsecond accuracy. That specification does not mention precision, thus this specification avoids use of precision for these date-time values as well. Note that a USS may have human-interface systems that display times in other formats and this is not in conflice with this specfiication.

A USS MUST reject any data submission wherein any time value fails to meet the API specification. This means that any other time format is unacceptable to a USS. FIMS will also reject data submissions with incorrectly formatted time values.

Altitudes

All altitudes within UTM are expected to be in reference to World Geodetic System 1984 [WGS 84]. *To convert between feet and meters, the USS MUST use a factor of 0.3048 m/ft.* This conforms to the definition of an "international yard" as discussed in [FRDoc59-5442], and is therefore used to define the "international foot". This conversion is necessary given the default units of meters within WGS84 and to provide improved interoperability within the National Airspace System.

Time Synchronization

A common reference to time is of high importance within the USS Network and within UTM as a whole. Time sync solution TBD, for TCL3 testing we may just require documentation on how the USS servers and the clients to a USS are kept in time sync. During checkout we may check for drift or require a specific intermediate solution for time synchronization.

Operator Support

The major role of a USS is to support UAS operators in performing their missions. To be a USS implies at least a minimal level of functionality provided to UAS operators. A USS is considered to be supporting an operation from the time the USS submits an authorization announcement or notification to FIMS and the USS Network on behalf of that operation. This support continues until well after the operation is completed or cancelled in that the USS can be asked for historical data on that operation. Requirements on this aspect to follow.

A USS MUST ensure that a UAS operator's plan conforms to published airspace rules and regulations. This will likely involve checking all elements of the plan and its components against an appropriate FAA rule or set of rules. For informative purposes, the following might be the types of checks that a USS performs for an operation plan (this list is not intended to be exhaustive and may not completely align with current rules and is for illustrative/discussion purposes only):

- A UAS operator intends to fly as a Part 101E operation. The USS should check (amongst other things) that it is VLOS, non-commercial, a nd whether it is or is not within five miles of an airport..
- A UAS operator intends to fly as a Part 107 operation. The USS should check (amongst other things) that the operation is VLOS, in Class G and/or designated airspace, and has a remote pilot in command (RPIC) with appropriate credentials.
- A UAS operator intends to fly as an operation under a future FAA rule: The USS should check all aspects of the operation to ensure it meets the requirements of the rule.

For certain types of operations under certain FAA rules (TBD), a USS might need to report the current state and position of the operation to a requesting party (another USS or FIMS/ANSP, for example). *For all operations, the USS MUST be able to report the state (as defined in the FIMSUSS-API) of the operation. For all non-Part 101E operations supported by the USS, the USS MUST be able to supply a current (within the last 2 seconds) position within 1 second of receiving an authorized request for that position.* Note that tracking of Part 101E (i.e., hobbyist) operations is not required, but tracking non-hobbyist operations is required.

A USS MUST supply operation information to a requesting operator associated with that operation. This requirement is related to the operator's right to access data related to its operation that is being shared within the UTM System and is being stored by the USS.

A USS MUST offer a mechanism to receive messages related to in-flight emergencies from a supported operation. A USS MUST acknowledge a message related to an in-flight emergency from a supported operation. An acknowledgement MAY be an appropriate HTTP status code response to the message. *A USS MUST notify its LUN of any operation under its management reporting an in-flight emergency.* Note that an operation that is reporting an in-flight emergency may actually be conforming with its plan and would not necessarily be in any other state than ACTIVE (see State Maintenance section).

A globally-unique flight identifier (GUFI) serves to uniquely identify an operation within UTM and, potentially, throughout the National Airspace System (NAS) as a whole. A GUFI is a UUID. *A USS MUST assign a GUFI for each supported operation. A USS MUST keep a GUFI constant once assigned to an operation.* It is acceptable to alter non-GUFI data per the appropriate APIs or to develop a new operation with the appropriate data while closing the previous operation. Operations with different GUFIs will be assumed to be different operations.

A USS MUST offer an automated mechanism for a client (UAS operator, another USS, FIMS, etc.) to inspect the status of the USS Instance. This mechanism will allow another stakeholder insight into the health of the USS Instance and have some level of confidence that its services are still available to the expected Quality of Service.

State Maintenance

A USS is responsible for maintaining a current record of the state of an operation. *A USS MUST report the valid state of an operation within 2 seconds of receiving a valid request for that state*. There are currently five states for operations that are recognized in communications between USSs and FIMS. These states are defined in the following table:

Operation State	Definition
ACCEPTED	The UAS Operation has become known outside of its own USS. The assumption of all stakeholders upon learning of a new ACCEPTED operation is that it meets all requirements to enter the airspace.
ACTIVATED	The UAS Operation is active and adhering to its requirements in accessing the airspace. The UAS Operation may not be airborne.
NON-CONFORMING	The UAS Operation was ACTIVATED, but is not adhering to its requirements in accessing the airspace.
ROGUE	The UAS Operation is no longer authorized in the airspace and must safely exit the airspace as quickly as practical. The UAS may not be under positive control.

CLOSED	The UAS Operation is no longer flying and will not fly again.

The following state diagram is informative of the acceptable state transitions.

Figure 4. UAS Operation state diagram.

A USS MUST maintain the state of an operation as ACCEPTED at all times from announcing it via the UTM APIs until it becomes ACTIVATED or CLOSED. A USS MUST maintain the state of an operation as ACTIVATED at all times from the start time of the operation until it is closed while it is in conformance with its plan and the rules of the airspace. A USS MUST transition an operation to the CLOSED state when it is no longer flying and will not fly again.

Conformance Monitoring

A USS is responsible for monitoring the conformance of UAS operations under its management. The level of management depends on the type of operation (Part 101E, Part 107, or Part 107X). Based on the mission of the UAS operator, the USS defines two sets of volumes. The first is a set of Conformance Volumes. At any given time, an operation is expected to be contained within at least one valid Conformance Volume. When defining this set of volumes, the USS should aid the UAS operator, perhaps by building off of the operator's planned flight path or mission description. Again, the expectation of all stakeholders within UTM is that any operation is maintained within at least one valid Conformance Volume at all times. Each Conformance Volume is contained (4 dimensionally) within an Operation Volume. It is the set of Operation Volumes that is included as part of the Operation data supplied to other UTM components via the appropriate APIs. The USS should make an effort to size of these volumes such that the impact on other users of the airspace is minimized. TBD: Are there requirements on the maximum 4D dimensions of Conformance Volumes? A conformance volume is not communicated during any phase of a nominal operation with FIMS or other USSs. Conformance Volumes may be requested by the ANSP in conjunction with an audit or investigation per the data Accounting and Auditing specification for a USS. The discussion in this paragraph supports the following requirement. *A USS MUST define a Conformance Volume for each Operation Volume for each operation. A Conformance Volume MUST be contained in all four dimensions within its associated Operation Volume.*

NON-CONFORMING operations should be a rare event. ROGUE operations should be even rarer! The USS is critical in ensuring that operators understand their Operation Volumes and necessity of staying within them, including the need to stay within their Conformance Geographies to minimize the number of NON-CONFORMING operations. In addition, the rate of NON-CONFORMING and ROGUE operations managed by a USS may become part of the Quality of Service metrics for a USS.

All of the "announcements" described through the end of this subsection imply following the current, relevant API documentation. Specifically, the [FIMSUSS-API] and the [USSREQ-API].

A USS MUST be aware within 1 second that an operation under its management is out of conformance. Note that 1 second is somewhat arbitrary at this point. This may be achieved through regular position reporting. This may be achieved through a messaging system between the USS and operators. This may be achieved through some other means. *The USS MUST maintain a record of the state of a non-conforming operation as NON-CONFORMING.*

A USS MUST announce to its LUN a non-conforming operation within 2 seconds of transitioning an operation into the NON-CONFORMING state. A USS MUST designate the state of an operation that has been in the NON-CONFORMING state for 30 continuous seconds as ROGUE. A USS MUST announce a ROGUE operation within 2 seconds of transitioning that operation to the ROGUE state. A USS may transition an operation to the ACTIVE or CLOSED states from the NON-CONFORMING state when the operation meets the requirements of those state definitions. *A USS MUST NOT transition a ROGUE operation to any state other than CLOSED. The USS MUST change the state of a ROGUE operation to CLOSED when that operation has ceased operating and not before it has ceased operating.* Essentially this pair of constraints implies that a ROGUE operation has no option other than to become CLOSED. *A USS MUST designate the state of an operation that has transitioned to the NON-CONFORMING state more than 3 times as ROGUE.* This requirement is in place due to the operation demonstrating its inability to adhere to its assigned conformance geography.

Contingency Management

Per the [USSREQ-API], an Operation contains a set of Contingency Plans. Each plan lists a non-empty set of causes, each with a single response. The Contingency Plan provides a pre-flight method to communicate how various unplanned situations might be handled by an operation. *A USS MUST provide at least one Contingency Plan per Operation Volume within an Operation plan as defined per the [USSREQ-API]. When a Contingency Plan is put into action, the USS MUST post an Alert Message containing the Contingency Plan to each other USS in its LUN. A USS MUST update the LUN via an Alert Message when any Contingency Plan ends or changes*. If an update to the operation plan is needed to support a contingency plan (e.g., a "return to base" may require updated operation volumes and/or times), then the USS will support such planning through the existing facilities and requirements described in this document.

USS-USS Communication

Collaboration is a key feature of the UTM System. To successfully collaborate, the communication between USSs is described here. *A USS Instance MUST implement the [USSREQ-API]*. This API standardizes the expectations of the communication methods to be provided by each USS Instance.

Operation Announcement

A USS Instance MUST announce a new Operation via the [USSREQ-API] to all USS Instances that intersect that new Operation. Currently, this is achieved via an HTTP POST to the /operations endpoint of each of those intersecting USS Instances, though this document defers to the current [USSREQ-API] for the correct mechanism.

Position Reports

A USS MUST collect position updates from all ACTIVE Part 107X operations. A USS MUST provide access to all Part 107X operation position updates to FIMS upon request per the [USSREQ-API]. A USS MUST provide access to position updates for a Part 107X operation (Operation A) to another USS upon request when that second USS has an active operation with an operation volume intersecting Operation A's operation volumes. In simpler words: if you have a operation crossing another USS's operation, you need to exchange position data with each other upon request. This document defers to [USSREQ-API], however as of this writing, the position updates are provided as WebSocket connections. This implies a publish-subscribe paradigm to access position information. These subscriptions may be "firehose" style wherein all positions for all operations for a USS Instance are provided out of one subscription, or "server-side filtered" wherein positions for a single operation are provided for each established subscription.

A USS MUST provide access to position updates (if available) to its LUN for all operations in the ROGUE or NON-CONFORMING states. This is for safety awareness.

Negotiation

There will be occasions wherein planned operations managed by one USS are intersecting (four-dimensionally speaking) with planned operations for another USS. In this case, a negotiation between the USS Instances is required. If there are operations managed by the same USS (perhaps within separate USS Instances), the assumption is that a negotiation occurs internal to the USS and that the intersecting operations will be executed safely.

The specification for negotiation needs further development. Currently the requirement will be explicit acknowledgement from both USS Instances as to their awareness of the intersecting operation plans. At that point, a USS may decide to alter the plans of its managed operation or both operations may proceed as planned following the established rules for the airspace in terms of keeping safe. Basically this means that both USSs agree that unmanned aircraft (UA) associated with their operations will not hit each other. Questions regarding legal liability are out of scope for this document.

A USS MUST send a message according to the [USSREQ-API] to another USS within 2 seconds of recognizing an operation plan managed by the first USS intersects an operation plan of the second USS. Upon receiving a message regarding an intersecting operation plan from another USS, a USS MUST send an acknowledgement message per the [USSREQ-API] to that other USS.

Communication with FIMS

A USS is expected to communicate with FIMS through Internet connections. *A USS MUST communicate with the FIMS-OPS server as specified in the [FIMSUSS-API]*.

Accounting and Auditing

This section contains a summary of the accounting and auditing requirements of a USS. These are related to the retention of operational data in terms of which data need to be stored for what period of time as well as who would be allowed access to those data and under what circumstances.

Prior to non-hobbyist flight, a USS MUST do the following:

- *Obtain a digital signature of an operation plan by the RPIC for that operation.*
- *Obtain a digital signature of an operation plan by the vehicle for that operation.*
- *Obtain a copy of the valid Performance Authorization, if any, under which that operation will be performed.*

The signing of an operational plan by a vehicle and an RPIC provides assurance that the resources noted within the operational plan are indeed the resources to be used in execution of the plan. This is a non-repudiation and data integrity step. RPICs will have confidence that plans are not

altered after they have signed/agreed to serve as RPIC. UAS operators and USSs will have confidence that an RPIC will not be able to claim they were not part of the operation. Similar arguments can be made for the vehicle: all stakeholders will have confidence regarding the exact vehicle performing an operation. Note that plans can be approved before signing takes place as this allows for some last minute alterations in the involved parties to support a variety of use cases.

A USS will have requirements for storing logs of queries and connections to its systems. Details, including formats of the logs and the length of time that they need to be kept, are to be determined.

Rios, Joseph (ARC-AFO), for C&N RTT support, we should require USS to collect contextual/experiential and digital data once ROGUE state is declared. Examples of these data include off-nominal situation report form if encountered, UA state history for the last 90 (this can change) seconds, USS-UAS operator data exchange records for the last 90 seconds, etc.

USS Quality of Service

A USS is a critical component in the UTM System. In some scenarios, the USS is a safety-critical component. As such, there are requirements for overall Quality of Service (QoS) that need to be maintained by each USS Instance. This section captures those QoS elements not captured elsewhere in this document. The QoS metrics are TBD.

1. Non-conforming operation rate per day/week/month?
2. Rogue operation rate per day/week/month?
3. Planned operation volume utilization rate (needs to be above some percentage?)

Authorization Revocation

In the event that a USS is deemed to be out of specification, its ability to request authorization tokens from FIMS-Authz may be revoked. This may occur if the service provided by the USS is not meeting the QoS requirements. This may occur if the USS is not adhering the communication protocols within the USS Network.

USS Checkout Process

An organization interested in offering services as a USS within the UTM System needs to complete a checkout process. The requirements that are checked during this process are those that are included in this specification. Since each requirement is not necessarily a software-specific requirement, an entity can expect a combination of software testing of their USS implementation along with required supporting documentation and other artifacts. Upon successful completion of this checkout process, the organization will be recognized as a valid USS. An identity will be provisioned for the USS within the UTM System. That identity will be managed within FIMS. The checkout process is managed by the Air Navigation Service Provider (ANSP), but might be executed by an entity other than the ANSP at the discretion of the ANSP.

A potential flow to complete the checkout process may include the following steps for the interested entity:

1. Review USS documentation.
2. Implement USS per USS Specification.
3. Test implementation using an existing "sandbox" environment (not currently in existence as of writing).
4. Apply for checkout process.
5. Complete checkout.
    a. Software checkout
6. Obtain identity information from ANSP/FIMS.

Further detail or formalization is currently beyond the scope of this document.

Step 6 above will follow [NIST.800.63.3] Digital Identity Guidelines. USS identities in the UTM System will be assured according to the following levels in [NIST.800.63.3]:

1. Identity Assurance Level 3 (IAL3)
2. Authenticator Assurance Level 3 (AAL3)
3. Federation Assurance Level 3 (FAL3)

These Assurance Levels are obtained by considering the "Maximum Potential Impacts for Each Assurance Level" as presented in [NIST.800.63.3]. Simply described, if any of the listed Impacts is "High" for an Assurance Level, then the Assurance Level needs to be assigned Level 3. While multiple Impacts may be considered "High" for each Assurance Level, the "inconvenience, distress, or damage to standing or reputation" and "harm to agency programs or public interests" could be argued to be "High" for each Assurance Level. In the future, a more detailed analysis of these categorizations will be provided in a separate document. A separate document (or set of documents) will further detail the USS identity assurance system within UTM.

Threat Model

This section will contain a summary of the identified threats against a USS or USS Instance.

Certificate Authority Compromise

PROBLEM: There have been documented attacks and flaws with traditional Certificate Authorities. If UTM relies solely on traditional CAs, there is the risk that communications could be compromised and that data becomes suspect within the system.

MITIGATION: Two layer CA.

References

Identifier	Reference
Internet Engineering Task Force Documents	
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, DOI: 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.
[RFC4122]	Leach, P., Mealling, M., Salz, R., "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI: 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.
[RFC5246]	Dierks, T., Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 6749, DOI: 10.17487/RFC5246 , August 2008, <https://www.rfc-editor.org/info/rfc5246>.
[RFC6749]	Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI: 10.17487/RFC6749 , October 2012, <https://www.rfc-editor.org/info/rfc6749>.
[RFC6750]	Jones, M., Hardt, D., "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, DOI: 10.17487/RFC6750 , October 2012, <https://www.rfc-editor.org/info/rfc6750>.
[RFC7515]	Jones M., Bradley J., Sakimura N., "JSON Web Signature (JWS)", RFC 7515, DOI: 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.
[RFC7519]	Jones M., Bradley J., Sakimura N., "JSON Web Token (JWT)", RFC 7519, DOI: 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.
[RFC7662]	Richer, J., Ed. "OAuth 2.0 Token Introspection", RFC 7662, DOI: 10.17487/RFC7662, October 2015, <https://www.rfc-editor.org/info/rfc7662>.
[RFC8017]	Moriarty, K., Kaliski, B., Jonsson, J., Rusch, A., "PKCS #1: RSA Cryptography Specifications Version 2.2", November 2016, <https://www.rfc-editor.org/info/rfc8017>.
National Institute of Standards and Technology Documents	
[NIST.800.57.p1]	Barker, E., "Recommendation for Key Management, Part 1: General", NIST Special Publication 800-57 Part 1 Revision 4, January 2016, <http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>.
[NIST.800.57.p2]	
[NIST.800.57.p3]	
[NIST.800.63.3]	https://pages.nist.gov/800-63-3/
[NIST800.90A.R1]	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
[NIST800.90A.R1.LIST]	http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html
UTM Application Programming Interface Specifications	
[USSDS-API]	https://app.swaggerhub.com/apis/utm/ussdiscovery/v2
[FIMSAuthzAPI]	https://app.swaggerhub.com/apis/utm/fims_authz/v1

[FIMSUSS-API]	https://app.swaggerhub.com/apis/utm/fims/v2
[USSREQ-API]	https://app.swaggerhub.com/apis/utm/uss/
Other Documents	
[UTMGlossary]	TBD. may want a dedicated NASA TM just on this element for reference to ourselves and all stakeholders
[NASASysEng]	"NASA Systems Engineering Handbook Rev. 2", Feb 2017, <http://hdl.handle.net/2060/20170001761>
[UTMConOps]	Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., Robinson III, J., "Unmanned Aircraft System Traffic Management (UTM) Concept of Operations", AIAA Aviation Forum 2016, June 2016
[RSA]	Rivest, R., Shamir, A., and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Volume 21, Issue 2, pp. 120-126, DOI 10.1145/359340.359342, February 1978.
[CCADB]	<https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport>
[MOZROOT]	"Mozilla Root Store Policy", version 2.5, accessed 20-07-2017, <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>
[ITUX667]	ITU, "Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers", Edition 3.0, October 2012, <http://handle.itu.int/11.1002/1000/11746>.
[OpenAPIv2]	https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md
[JSONSpec]	https://tools.ietf.org/html/draft-wright-json-schema-01
[ISO8601]	ISO - International Organization for Standardization, "Data Elements and Interchange Formats - Information Interchange - Representation of Dates and Times - Third Edition", December 2004, <https://www.iso.org/iso-8601-date-and-time-format.html>.
[WGS84]	http://earth-info.nga.mil/GandG/wgs84/index.html
[FRDoc59-5442]	National Bureau of Standards, "Refinement of Values for the Yard and the Pound", June 1959, F.R. Doc. 59-5442, <https://www.ngs.noaa.gov/PUBS_LIB/FedRegister/FRdoc59-5442.pdf>.

Future References (TBD and other Orange Notes)

Document/Element	Description

Summary of Requirements

This section is provided for convenience. All of the requirements described in the main text of this document are summarized in the table below. For common reference, each requirement is provided a unique identifier.

Req. ID	Requirement	Specification Section
UTM-USS-001	*As part of the checkout process, the applying organization MUST generate a public-private key pair (UTM-PUBLIC-KEY and UTM-PRIVATE-KEY) using the RSA approach [RFC8017][RSA].*	
UTM-USS-002	*The applying organization must supply the generated UTM-PUBLIC-KEY to the UTM regulator.*	

UTM-USS-003	*The organization MUST obtain a public certificate (INTERNET-PUB-CERT) from a certificate authority within the Common CA Database [CCADB] that as a geographic focus that includes "USA".*	
UTM-USS-004	*When generating a random number for any purpose within the UTM System, a USS MUST use a method adhering to the recommendations in [NIST800.90A.R1].*	
UTM-USS-005	*When generating a UUID, a USS MUST generate a version 4 UUID as per [RFC4122].*	
UTM-USS-006	*For any exchange of JSON-formatted data, the receiver MUST ignore the received data whenever any required field (as specified in the relevant schema definition) is missing or malformed.*	
	If missing/malformed data are received via a RESTful call, the receiver MUST reply with an HTTP 400 status code.	
UTM-USS-007	*A USS MUST obtain an access token from the FIMS Authorization Server using the published [FIMSAuthzAPI].*	
UTM-USS-008	*Authentication of the USS with the FIMS Authorization Server MUST be completed via TLS 1.2 client authentication using the USS INTERNET-PUB-CERT*.	
UTM-USS-009	*The USS MUST be able to decode a properly formatted JWT.*	
UTM-USS-010	*The USS MUST be able to check a JWS for validity*.	
UTM-USS-011	*A USS MUST NOT accept a JWT when the current time is greater than the "exp" claim value in the JWT.*	
UTM-USS-012	*A USS MUST NOT accept a JWT when the current time is earlier than the "nbf" claim value of the JWT.*	
UTM-USS-013	*A USS MUST NOT accept a JWT wherein the "iss" claim does not match the URL of the FIMS Authorization Server.*	
	A USS MUST NOT accept a JWT wherein the scope is insufficient for the resource being requested.	
	A USS MUST NOT accept a JWT wherein the "sub" claim cannot be mapped to the data provided on a submission.	
	A USS MUST exclusively support token exchange via the Authorization Request Header Field as per [RFC6750] Section 2.1.	