NASA/TM-2019-220376

UAS Service Supplier Specification

Baseline requirements for providing USS services within the UAS Traffic Management System

Joseph L. Rios
Ames Research Center, Moffett Field, California

Irene S. Smith
Ames Research Center, Moffett Field, California

Priya Venkatesen
SGT Inc., Moffett Field, California

Jeffrey R. Homola
Ames Research Center, Moffett Field, California

Marcus A. Johnson
Ames Research Center, Moffett Field, California

Jaewoo Jung
Ames Research Center, Moffett Field, California

October 2019

NASA/TM-2019-220376

UAS Service Supplier Specification

Baseline requirements for providing USS services within the UAS Traffic Management System

Joseph L. Rios
Ames Research Center, Moffett Field, California

Irene S. Smith
Ames Research Center, Moffett Field, California

Priya Venkatesen
SGT Inc., Moffett Field, California

Jeffrey R. Homola
Ames Research Center, Moffett Field, California

Marcus A. Johnson
Ames Research Center, Moffett Field, California

Jaewoo Jung
Ames Research Center, Moffett Field, California

National Aeronautics
and Space Administration

Ames Research Center
Moffett Field, California 94035-1000

October 2019

Acknowledgments

This was a working document for nearly three years as the NASA UTM Project developed the UTM System and concept with its partners, with earlier forms dating back even further. Valuable feedback and testing enabled the document to get to its current level of maturity. We thank all of our partners who built software to this specification and tested with us in simulation and in flight.

This report is available in electronic form at

https://www.sti.nasa.gov

Table of Contents

1. Introduction

UTM has the stated goal of providing safe, efficient, and fair access to the low-altitude airspace for small Unmanned Aircraft Systems (sUAS). The management of these sUAS operations is envisioned to take a different form than the management of traditional aviation in the National Airspace System (NAS). In UTM, management of the airspace is a partnership between the Air Navigation Service Provider (ANSP) and the users of the airspace. Some of the key services that might have been provided by the ANSP for traditional aviation are provided instead by a federated set of UAS Service Suppliers (USS). A new, UTM-specific component that is implemented on the ANSP side for this system is called the Flight Information Management System (FIMS). This federated, collaborative approach to airspace management supports several key properties of the UTM System including scalability, enabling more seamless evolution, partitioning sUAS management from traditional aviation, and others. For a comprehensive description of the UTM System, both versions of the Concept of Operations ([UTM_ConOps_NASA] and [UTM_ConOps_FAA]) provide the primary starting points.

The NASA ConOps ([NASAConOps]) document is an initial description of the concept and NASA's approach to building and testing that concept. The FAA UTM ConOps ([FAAConOps]) document is an evolution and update of NASA's concept with a focus on use cases. For a deeper dive on the UTM Concept, details are deferred to those two documents.

To provide an overview of what a USS is, the following is an excerpt from [FAAConOps]:

> *A USS is an entity that provides services to support the safe and efficient use of airspace by providing services to the Operator in meeting UTM operational requirements. A USS:*
>
> 1. *acts as a communications bridge between federated UTM actors to support Operators' abilities to meet the regulatory and operational requirements for UAS operations, and*
> 2. *provides the Operator with demand forecasts for a volume of airspace so that the Operator can ascertain the ability to efficiently conduct their mission, and*
> 3. *archives operations data in historical databases for analytics, regulatory, and Operator accountability purposes.*
>
> *In general, these key functions allow for a network of USSs to provide cooperative management of low altitude operations without direct FAA involvement. USS services support operations planning, aircraft de-confliction, conformance monitoring, and emergency information dissemination. USSs may also work, if applicable, with local municipalities and communities to gather, incorporate, and maintain airspace restrictions and local airspace rules into airspace constraint data (e.g., preemptive airspace). USSs may also provide other value-added*

> *services to support UTM participants as market forces create opportunity to meet business needs. See Appendix D for a more detailed description of a USS.*

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.

The collection of USSs working to manage the airspace within the UTM Concept is called the “USS Network.” For a more formal definition, this document defers to the [UTMGlossary].

This document is primarily targeted at implementers of USS systems, though it may be informative to other stakeholders within UTM.

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

This document is a research artifact from the NASA UTM Project. It is intended to facilitate convergence on the concept, allow for implementation of interoperable test systems, and lay the groundwork for a future, formal specification. This is not a formal standard.

2. 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. A summary of the requirements is provided at the end of the document.

Requirements that are currently assumed to be needed, but are not yet defined, are marked by a superscript tag in the text. A summary of these tags is provided at the end of the document.

3. Terminology

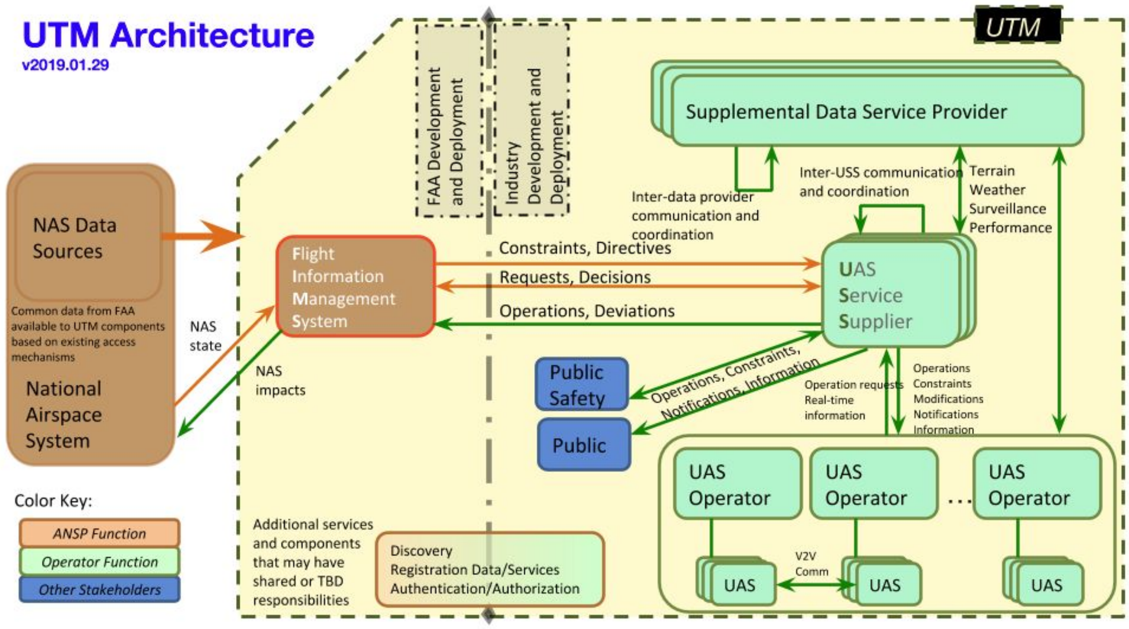
A USS is discussed with an active voice, as if it is an organization or entity, when in reality it is a collection of software, services, and interfaces. When a statement such as "A USS may do this" is made, it is understood to mean that "A software implementation adhering to the USS Specification may be implemented to do this." This is a stylistic choice for the goal of clarity.

For lack of other current terminology, all small UAS (sUAS) operations that would require a waiver under Part 107 (i.e., commercial operations) or require a waiver under Part 101, Subpart E (i.e., hobbyist operations also called "Part 101E") will be called "Part 107X operations" until there is a more appropriate term or rule introduced. All operations that are not flown under Part 101, Subpart E will be referred to as “non-hobbyist operations” in this document.

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

4. USS Overview

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



UTM Architecture
v2019.01.29
UTM
FAA Development and Deployment
Industry Development and Deployment
Supplemental Data Service Provider
Inter-data provider communication and coordination
Inter-USS communication and coordination
Terrain
Weather
Surveillance
Performance
NAS Data Sources
Common data from FAA available to UTM components based on existing access mechanisms
National Airspace System
NAS state
NAS impacts
Flight Information Management System
Constraints, Directives
Requests, Decisions
Operations, Deviations
UAS Service Supplier
Public Safety
Public
Operations, Constraints, Notifications, Information
Operation requests
Real-time information
Operations
Constraints
Modifications
Notifications
Information
UAS Operator
UAS Operator
. . .
UAS Operator
UAS
V2V Comm
UAS
UAS
Additional services and components that may have shared or TBD responsibilities
Discovery
Registration Data/Services
Authentication/Authorization
Color Key:
ANSP Function
Operator Function
Other Stakeholders

Figure 1. UTM Architecture.

The set of other USSs with which a USS are required to communicate are said to be that USS's Local USS Network or LUN[1]. The concept of a LUN is important in the definition of requirements within this document.

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.

5. Authority to Operate

This document is designed to be a reference for stakeholders in the future UTM System as it is targeted for deployment in the United States. However, there will be wider applicability of the information contained herein. As such, details regarding risk management and software assurance are not provided, as these requirements will need to be appropriately tailored. From the NASA UTM Project's perspective, however, there are some high-level principles that should be applied to USSs seeking to collaboratively manage traffic in the U.S. National Airspace System. Requirements in this regard lead to a USS's authority to operate as a USS within UTM. Overall, this document focuses on the requirements related to operation, not on the full requirements to gain an authority to operate.

NASA makes the assumption that the airspace regulator will determine the classification of data that will be handled and exchanged within the USS Network and between USSs and FIMS. Likely this categorization will follow federal guidelines and leverage the initial step of the Risk Management Framework, as detailed in [FIPS199]. At a high level, that document describes how to categorize data at one of three levels (low, medium, or high) on three axes (confidentiality, integrity, and availability). Information may be further categorized in terms of Personally Identifiable Information and privacy (which is different than confidentiality in that privacy exclusively focuses on information related to individuals).

Short-cutting some of the details of the Risk Management Framework, this categorization process leads to a set of "controls" on an information system that can be translated into requirements, or formalized in other ways. For details on these controls and how they might be assured, [NIST800.53] and [NIST800.53A] are key references. Each USS would be required to show how they implement the various controls. It is valuable to note that some of the controls might be met through proper implementation of certain requirements herein. For example if timestamping and clock synchronization

[1] Depending on how discovery and other elements are defined within a deployment of UTM, every USS's LUN will be different. Consider the relationship '~' where '~' means "has in its LUN." For example, "USS A has in its LUN USS B" implies "USS B has in its LUN USS A." This makes the relationship symmetric. However "USS A has in its LUN USS A" is NOT true since it would lead to implications of USS A needing to communicate with itself to satisfy the requirements of this document. So, the relationship is not reflexive. Finally, (USS A ~ USS B) and (USS B ~ USS C) does not imply that (USS A ~ USS C), thus the relationship is not transitive. It is uncommon to find real-world relations that are not reflexive, not transitive, but are symmetric, thus this observation deserves a footnote.

are implemented as required in this document, that may satisfy control number AU-8 in [NIST800.53] (“Timestamps”), depending on the bounds placed on synchronized time via that control.

In addition, many of the controls in the “Access Control” section of [NIST800.53] will be met through proper implementation of authentication and authorization as described in [UTMAuth].

So while this document does not attempt to align directly with the Risk Management Framework, it should be expected by stakeholders that USSs will be authorized only after satisfaction of a Risk Management Framework process. Appendix G of [NIST800.37r2] entitled “AUTHORIZATION BOUNDARY CONSIDERATIONS: COMPLEX SYSTEMS, APPLICATIONS, AND THE EFFECTS OF CHANGING TECHNOLOGIES,” describes the unique considerations of services provided by non-federal organizations on behalf of the government. The following excerpt from that section of NIST800.37r2] highlights the issues and considerations that arise in a proposed system like UTM where USSs are providing services under the purview of a federal agency:

> While the concepts of external systems and external service providers are not new, the current pervasiveness and frequency of their invocation can present organizations with significant, new challenges. There are instances where system elements, subsystems, or perhaps the entire system may be outside of the direct control of the organization that authorizes its operation…. FISMA and OMB policy require external providers that process, store, or transmit federal information or operate information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Federal security and privacy requirements also apply to external systems storing, processing, or transmitting federal information and any services provided by or associated with the external system.

As an initial requirement in this regard, this specification provides a single, high-level requirement:

[UTM-USS-001] A USS MUST meet the requirements of the authorizing entity for authority to operate as a USS.

To finalize this portion of this specification document, a final highlight related to internationalization is provided. The UTM Project would like to continue promoting international harmonization, so the reliance upon NIST documentation, if not acceptable to an ANSP, should not be a hindrance to adoption. NIST offers a mapping to ISO standards, including some gap analysis of that mapping.

6. API Requirements

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.

The API documentation is provided in a format such that code may be generated from the API. Currently the format is [OpenAPIv2.0].

[UTM-USS-002] All data exchanges via UTM APIs MUST be completed over a TLS-secured connection.

[UTM-USS-003] All TLS implementations for UTM data exchanges MUST conform to the most recent version of NIST 800-52.

As of this writing, the most current version of NIST 800-52 is a draft for revision 2 [NIST800.52v2]. Details related to the keys and certificates used in establishing such TLS connections are deferred to [UTMAuth].

The following is a brief overview of the APIs relevant to the USS Network.

6.1. FIMS-USS API

The [FIMSUSS-API] defines FIMS-specific data exchanges to FIMS from any USS. FIMS also implements the [USSREQ-API], but reserves the right to provide HTTP 40X status code responses for certain exchanges that are not applicable to FIMS. This approach allows USS implementers to interact with FIMS using the same endpoint names and models as they use to communicate with each other.

[UTM-USS-004] A USS MUST communicate with FIMS per the [FIMSUSS-API] and the [USSREQ-API].

6.2. 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.

[UTM-USS-005] A USS MUST communicate with other USSs per the [USSREQ-API].

6.3. 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 as initially defined in [RFC6749]. 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-USS-006] A USS MUST use the [FIMSAuthzAPI] for authorization purposes with other USSs.

[UTM-USS-007] A USS MUST use the [FIMSAuthzAPI] for authorization purposes with FIMS.

6.3. Public Safety API

The [PUBSAFEAPI] provides the interface definition to support public safety functionality within the USS Network. This includes support of networked Remote ID[2].

[UTM-USS-008] A USS MUST implement the [PUBSAFEAPI].

7. Software Engineering Requirements

This section collects general software engineering requirements for USS implementation.

7.1. Random Numbers

Random numbers are a part of other requirements described in this document. [NIST800.90A.R1] describes methods of Deterministic Random Bit Generation and [NIST800.90A.R1.LIST] provides a list of validated implementations adhering to those methods.

[UTM-USS-009] 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].

Another informative reference is [RFC4086] (Randomness Requirements for Security) which describes Best Current Practices (as of 2005) in this regard.

[2] Note that the support for RemoteID may be considered a separate service that is not required for a nominal USS to directly support. If the decision to define RemoteID and potentially public safety functionality as separate services, then this section and associated requirement may be struck.

7.3. UUID Generation

The generation of Universally Unique Identifiers (UUIDs) is a necessary part of a USS operation.

[UTM-USS-010] When generating a UUID, a USS MUST generate a version 4 UUID as per [RFC4122].

Note that this requirement implies that the UUID is appropriately randomized and, therefore, will not be intentionally reused for any operational purpose. In some cases, known or repeated UUIDs aid in testing, but this use of UUIDs should be made clear to all participants in such testing.

7.4. JSON Data

Data exchanges within 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 [RFC8259] (though it does so as a previous version, [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 [RFC8259] will be the defining reference.

For clarity, the following requirements re-write and solidify JSON requirements from [RFC8259] that might be read as design decisions if taken as-is from that specification.

[UTM-USS-011] JSON text exchanged between USSs MUST be encoded using UTF-8.

[UTM-USS-012] JSON text exchanged between a USS and FIMS MUST be encoded using UTF-8.

UTF-8 (or Universal Transformation Format-8) is a text encoding standard described in detail in [RFC3629]. In the JSON standard, [RFC8259], this requirement of UTF-8 is written with the caveat that this encoding is required when the "systems are not part of a closed ecosystem." Thus, the requirements are stated here to avoid ambiguity. In addition, since the JSON specification has a "MAY" statement in that same section, that statement is hardened into a requirement for USS communication purposes here:

[UTM-USS-013] A USS MUST treat the presence of a byte order mark as a malformed data exchange.

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.

[UTM-USS-014] For any exchange of JSON-formatted data, the receiver MUST reply with an HTTP 400 status code whenever any required field (as specified in the relevant schema definition) of the received data is missing.

[UTM-USS-015] If malformed data are received via a RESTful call, the receiver MUST reply with an HTTP 400 status code.

An authoritative definition for “malformed” was not found by the authors, despite the term being regularly used in many computer science contexts. There are definitions available for well-formed, so malformed may be considered “not well-formed.” The simplest definition for “malformed” might be: data that do not meet the expected protocol or formatting. For example, data supplied as JSON but not using UTF-8 encoding should be considered “malformed” data.

[UTM-USS-016] A USS MUST NOT reject JSON due to the ordering of fields within the JSON.

This follows from the definition in [RFC8259] of a JSON object:

> *An object is an unordered collection of zero or more name/value pairs, where a name is a string and a value is a string, number, boolean, null, object, or array.*

as well as the following note in [RFC8259] related to interoperability:

> *JSON parsing libraries have been observed to differ as to whether or not they make the ordering of object members visible to calling software. Implementations whose behavior does not depend on member ordering will be interoperable in the sense that they will not be affected by these differences.*

7.5. Units of Measure

[UTM-USS-017] 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.

7.5.1. Date-Time Format

All date-time values exchanged within the USS Network will use [ISO8601] for formatting guidance.

[UTM-USS-018] A USS MUST use UTC time for all date-times exchanged with other USSs.

[UTM-USS-019] A USS MUST use UTC time for all date-times exchanged with FIMS.

[UTM-USS-020] All date-times supplied by a USS to another USS MUST follow the format pattern YYYY-MM-DDThh:mm:ss.sssZ.

[UTM-USS-021] All date-times supplied by a USS to FIMS MUST follow the format pattern YYYY-MM-DDThh:mm:ss.sssZ.

[UTM-USS-022] A USS MUST verify that time strings have the format YYYY-MM-DDThh:mm:ss.sssZ.

According to [ISO8601], the three fractional decimal places for seconds corresponds to millisecond accuracy. That specification does not mention the term "precision," thus this specification avoids use of the term "precision" for these date-time values as well. Note that a USS may have human-interface systems that display times in other formats and such design decisions are not in conflict with this specification. Also note that the API requirements listed earlier combined with these date-time formatting requirements imply that a USS will reject any data submission that includes date-times that do not follow the correct formatting.

It bears noting that interoperability is non-trivial if such prescriptive formatting is not provided to USSs. [ISO8601] is a standard, but it provides for many design decisions and great flexibility. Leaving too many options provides several avenues for issues with parsers, libraries, interpretations and other elements that may affect interoperability.

7.5.2. Altitudes

[UTM-USS-023] All altitudes within UTM MUST be in reference to World Geodetic System 1984 [WGS 84].

[UTM-USS-024] 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 WGS 84 and to provide improved interoperability within the U.S. National Airspace System (NAS). This conversion may also aid integration with other systems relying on metric units.

Note that many related systems and maps rely on Above Ground Level (AGL) and Mean Sea Level (MSL) measures. Many UAS utilize height above takeoff location for some functions. Given these practices for which there are no standard established procedures for small UAS operations, the USS Specification aims to minimize confusion and ambiguity at the potential cost of translation. The overall goal is to ensure that data exchanged within the USS Network is as unambiguous as possible. However, given that there will be translations to get to and from WGS84, further requirements for altitude reporting are required for the USS Network. These will include, but are not limited to, how and which elevation models are used as well as conversion methods for AGL and Mean Sea Level to WGS84. Discrepancies can cause safety hazards[tbd_alt].

7.6. Time Synchronization

A common reference to time is of high importance within the USS Network and within UTM as a whole. The time synchronization solution within UTM will be determined through further discussions and research. Expect further requirements in future releases of this document[tbd_time].

Due to the unresolved issues with time synchronization, USSs will need to restrict how they use timestamps from other systems. The [USSREQ-API] provides requirements on various timestamps. In general, these requirements focus on the internal consistency of a given instance of a particular model. More concretely, an example of these requirements might be ensuring that a pair of timestamps are ordered properly, such as a `time_measured` and a `time_submitted` pair may have a requirement in the API that `time_measured <= time_submitted`. However there is no requirement that a USS receiving such an instance of a model needs to check those timestamps against any of its own internal clocks. So the receiving USS cannot reject data if is seems that times are inconsistent with its own time.

8. USS Network

This section collects requirements for successful integration of a USS within the USS Network.

8.1. USS Authorization

Requirements related to Public Key Infrastructure, identity management, authentication, authorization, and related topics will be deferred to a separate document, "UTM Authentication and Authorization Framework" [UTMAuth]. This leads to the generalized requirement:

[UTM-USS-025] A USS MUST adhere to the requirements described in [UTMAuth].

The [FIMSAuthzAPI] allows for the request of access tokens to use in communications within the USS Network. Tokens can be re-used by the authorized party as many times as necessary prior to their expiration. Excessive token requests to the FIMS Authorization Server may have detrimental effects on the server, impacting performance of the USS Network as a whole. Thus, USSs need to implement various best practices in relation to token use and re-use. The following requirement encourages re-use of tokens while they are still valid.

[UTM-USS-026] A USS MUST NOT request tokens with duplicate parameters while it is in possession of a valid token with those parameters and a valid use time of at least 50% of its initial valid use time.

The “valid use time” in the requirement refers to the difference between the issue and expiration time. Thus if there is a valid use time of 30 minutes at time of issue, then that token should be reused (assuming it is still known to be secure) for at least 15 minutes before requesting another token with the same parameters. The phrase “with the same parameters” can be interpreted as having, say, the same scope and audience values. Essentially if the values in the token would allow access to a given resource, then it should be reused until at least half of its life is gone. Note that this does not prevent the request of multiple tokens at once, as long as they each provide different types of authorization (for example different scopes and audiences) with the USS Network.

[UTM-USS-027] A USS MUST ensure that its access tokens stored on its systems are inaccessible to external entities.

[UTM-USS-028] A USS MUST remove all traces of another USS’s valid access token from its systems after the token serves its purpose of authorizing appropriate access.

This requirement is intended to ensure that a USS is not storing another USS’s tokens, as they have no legitimate value to any USS other than the USS to which the token was originally issued, and to guard against abuse of token usage. Thus, it is best to ensure that tokens are not available for abuse in the first place.

8.2. USS Discovery

The concept of discovery amongst USSs and FIMS is an active area of research and development[3]. This specification will defer discovery requirements to a future document and will add this placeholder requirement:

[UTM-USS-029] A USS MUST adhere to the requirements for discovery as described in [UTMDisc].

[3] For historical reference, the NASA UTM Project recognized the need for a discovery system when the UTM architecture evolved to a federated system of USSs. NASA tested a simple discovery system in flight testing for TCL2. In TCL3, Project Wing (under Google’s parent company, Alphabet) introduced an industry-defined discovery mechanism called “InterUSS.” NASA requested additional features and requirements from Wing to make it suitable for TCL4 testing and that updated system was used for TCL4 flight testing. Based on the initial (“main line”) InterUSS system and the experience and features of NASA’s TCL4 version, the InterUSS platform as been upgraded and moved to a project under the Linux Foundation with broader industry support and more independent stewardship. The system has been demonstrated after TCL4 in Europe and in the U.S. by multiple industry partners. The standardization efforts underway are expected to make use of the InterUSS approach to discovery.

8.3. Response Performance

Several requirements in this document have a “deadline clause” indicating how quickly a USS needs to respond to certain requests. It may be more appropriate to add an additional performance clause to any requirement with a deadline clause. For example, a requirement that reads: “A USS MUST respond to event X within one second,” likely should be written as “A USS MUST respond to event X within one second *at least 95% of the time.”* This additional performance clause helps account for latency and other issues that may affect distributed systems, but further specification is reserved for future formalization of this specification[tbd_qos]. This note applies to all requirements with deadlines contained in this document. It may also be reasonable to consider a parallel requirement for each of these deadline requirements using the 99th percentile and a longer deadline.

9. 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[tbd_logging].

[UTM-USS-030] A USS MUST protect an operator's Personally Identifiable Information (PII) from unlawful and/or unintended disclosure.

Discussion and definition of PII is deferred to [NIST800.122]. Even though that document focuses on the US Federal definition of PII and its existence within federal systems, the document can be reasonably applied to UTM-specific data that may potentially exist on and exchanged between non-federal systems.

[UTM-USS-031] Prior to a non-hobbyist operation, a USS MUST ensure the vehicle designated for an Operation it is supporting is properly registered.

Note that USSs are not required to check the registration of vehicles supported by other USSs. In addition, it may be reasonable to assume that a USS would not be able to check the registration of vehicles supported by other USSs in nominal cases, as doing so would likely require a higher level of access to that registration system than is provided to a nominal USS.

[UTM-USS-032] 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 hobbyist (a.k.a. Part 101E) operation. The USS should check (amongst other things) that it is visual line of sight (VLOS), non-commercial, and 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/Air Navigation Service Provider (ANSP), for example).

[UTM-USS-033] A USS MUST supply a position report from within the last 2 seconds for any non-hobbyist operation supported by that USS within 1 second of receiving an authorized request for that position.

Note that this document uses "position report" as a standalone set of data elements describing a single position exchanged in a single transaction, while "position tracking" as a set of position reports for a single operation provided in a single transaction (potentially a pub-sub transaction over a period of time) or over multiple transactions. Note that the ability to provide position tracking of hobbyist and Part 107 operations is not required, but the ability to provide position tracking of Part 107X operations is required. Further details on position reporting are provided in the Position Reports section.

[UTM-USS-034] When requested, a USS MUST supply operation information to the requesting operator associated with that operation.

This requirement is related to the operator's right to access data related to its operation as it is being shared within the UTM System and is being stored by the USS. Note that this requirement exists since the view of an operation is likely quite different depending on perspective (operator vs. USS, for example).

[UTM-USS-035] A USS MUST offer a mechanism to receive messages related to in-flight emergencies from a supported operation.

[UTM-USS-036] 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. 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 ACTIVATED (see State Maintenance and In-flight Emergency sections).

A globally unique flight identifier (GUFI) serves to uniquely identify an operation within UTM and, potentially, throughout the NAS as a whole. A GUFI is a UUID, which aids interoperability with the Flight Information Exchange Model. Specifically, note the formatting definition of a GUFI in the FIXM 4.1 schema.

[UTM-USS-037] A USS MUST assign a GUFI as a UUIDv4 for each supported operation.

[UTM-USS-038] 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.

There will be mechanisms to allow insight into the health of a USS to aid in monitoring expected Quality of Service (QoS) requirements. This is deferred to the [USSREQ-API] which is already a requirement for implementation. Note the endpoints for such monitoring are not currently defined in the [USSREQ-API], but would be needed in an operational system.

9.1. State Maintenance

A USS is responsible for maintaining a current record of the state of an operation.

[UTM-USS-039] A USS MUST report the valid state of an operation within 2 seconds of receiving a valid request for that state.

There may be future requirements on logging/persisting all state transitions for an operation and maintaining those logs for some period of time. There are currently six states for operations that are recognized in communications between USSs and FIMS. These states are defined in the following table:

Table 1. UAS Operation States.

Operation State	Definition
PROPOSED	*The UAS Operation has become known outside of its own USS but there are requirements to operate that have not yet been met. This is a time-limited state.*
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 or may not be airborne.*
NONCONFORMING	*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:

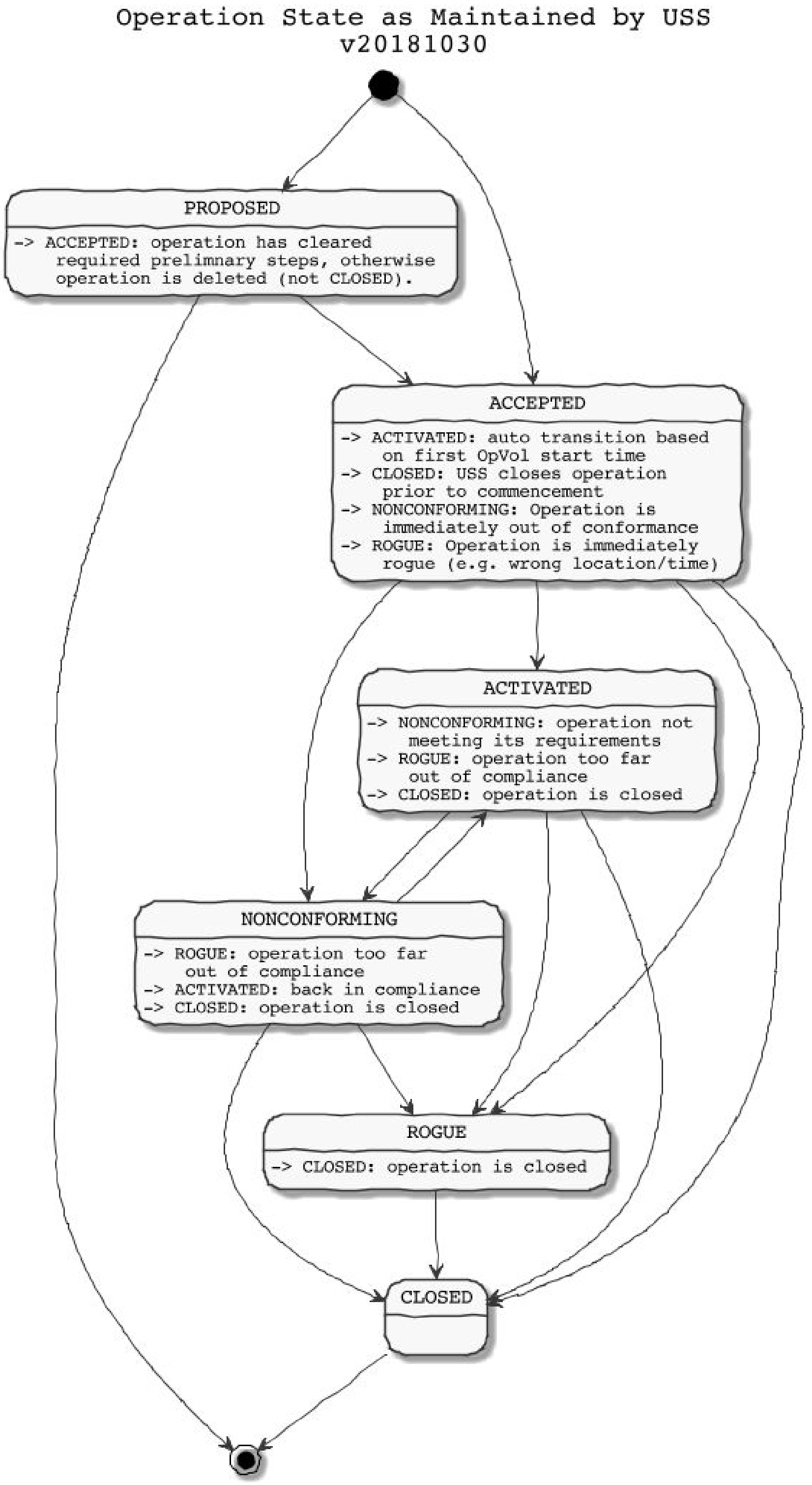

Operation State as Maintained by USS
v20181030
PROPOSED
-> ACCEPTED: operation has cleared required prelimnary steps, otherwise operation is deleted (not CLOSED).
ACCEPTED
-> ACTIVATED: auto transition based on first OpVol start time
-> CLOSED: USS closes operation prior to commencement
-> NONCONFORMING: Operation is immediately out of conformance
-> ROGUE: Operation is immediately rogue (e.g. wrong location/time)
ACTIVATED
-> NONCONFORMING: operation not meeting its requirements
-> ROGUE: operation too far out of compliance
-> CLOSED: operation is closed
NONCONFORMING
-> ROGUE: operation too far out of compliance
-> ACTIVATED: back in compliance
-> CLOSED: operation is closed
ROGUE
-> CLOSED: operation is closed
CLOSED

Figure 2. UAS Operation State Diagram.

[UTM-USS-040] A USS MUST maintain the state of an operation as ACCEPTED at all times from announcing it via the UTM APIs until an event causes a transition to another state.

[UTM-USS-041] A USS MUST maintain the state of an operation as ACTIVATED at all times after the start time of its first operation volume until it is closed while it is in conformance with its plan and the rules of the airspace.

Note that an operation is considered "active" from the begin time for its first operation volume until it is in the CLOSED state. Using this definition, an operation may be "active" but not in the ACTIVATED state due to, say, non-conformance or other issues.

[UTM-USS-042] A USS MUST transition an operation to the CLOSED state when it is no longer flying and will not fly again.

[UTM-USS-043] A USS MUST announce any transition to the CLOSED state to its LUN.

Small UAS operations may frequently land and takeoff. They may also swap batteries and perform other maintenance during an operation. To meet the position and state reporting requirements, a USS would need to account for these activities during an operation. A specific example highlighting potential complexity would be the battery swap during an operation. During the swap, telemetry from the UA to the GCS would not be available, thus interrupting the typical flow of positions from UAS to USS. But the USS may receive a request for the operation position during this time, so the USS would need some method to appropriately reply.

9.2. 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 (hobbyist, 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. In Figure 3, this is depicted with the “Flight Volume” box, but this can be any reasonable representation for the operator and the USS (waypoints, volumes, trajectories, etc.), with the key being that what the operator is planning to do is within a Conformance Volume. 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 (four-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 these volumes such that the impact on other users of the airspace is minimized. There will be requirements on the maximum 4D dimensions of Operation Volumes and Conformance Volumes [tbd_vols]. 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. The discussion in this paragraph supports the following requirements:

[UTM-USS-044] A USS MUST define a Conformance Volume for each Operation Volume for each operation.

[UTM-USS-045] A Conformance Volume MUST be contained in all four dimensions within its associated Operation Volume.

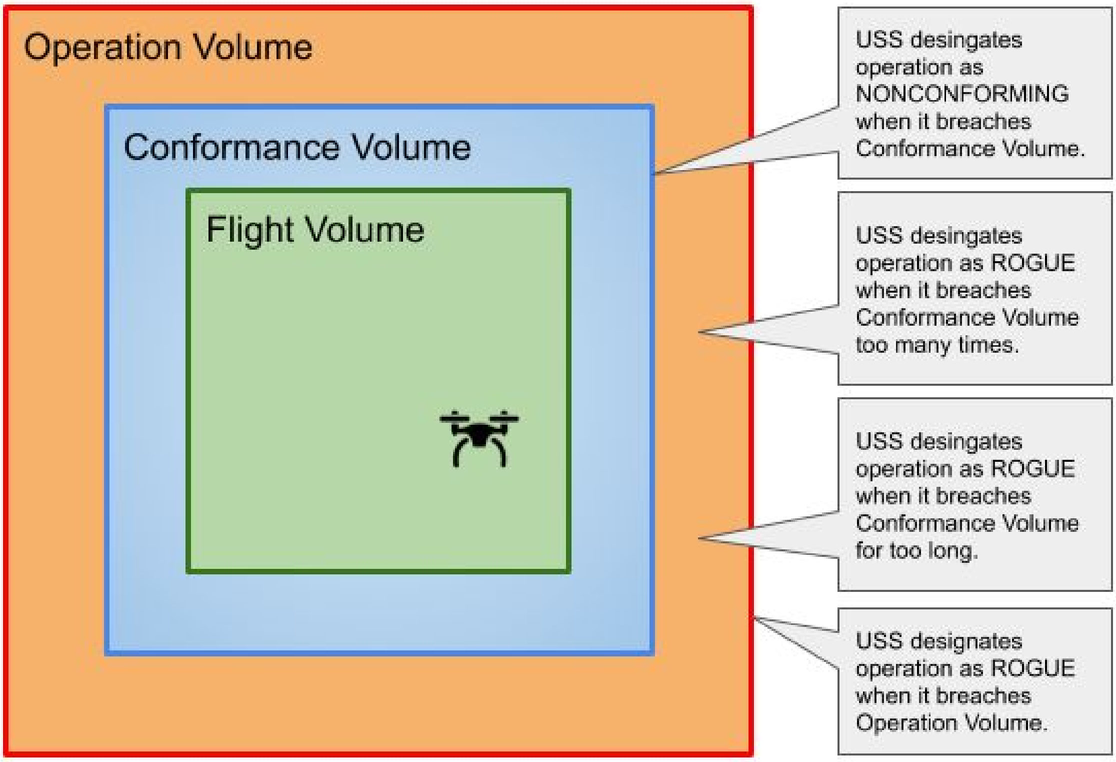

Operation Volume
Conformance Volume
Flight Volume
USS desingates operation as NONCONFORMING when it breaches Conformance Volume.
USS desingates operation as ROGUE when it breaches Conformance Volume too many times.
USS desingates operation as ROGUE when it breaches Conformance Volume for too long.
USS designates operation as ROGUE when it breaches Operation Volume.

Figure 3. Relationship of various volumes and state transitions.

An operation may become NONCONFORMING for reasons other than breaking its planned volumes. This is the definition currently provided by the [UTMGlossary], which may evolve as the overall UTM concept evolves:

> *Conformance:*
>
> *A property of a UAS operation denoting adherence to the submitted plan, the rules of the airspace, and the required data exchanges during operation. Specific, non-comprehensive requirements for maintaining conformance are as follows:*
>
> 1. *Staying within conformance volumes.*
> 2. *Submitting position reports at required rate.*
> 3. *Responding to required information requests from USS.*
> 4. *Meeting agreed requirements for operation. Examples (non-comprehensive):*
>   a. *Surveillance coverage*
>   b. *Weather limits*

c. *Visibility condition*

When an operation is no longer in conformance, that operation is deemed nonconforming and will be placed in the NONCONFORMING state by the USS. NONCONFORMING 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 Volumes to minimize the number of NONCONFORMING operations. In addition, the rate of NONCONFORMING and ROGUE operations managed by a USS may become part of the QoS 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]).

[UTM-USS-046] A USS MUST be aware within 1 second that an operation under its management is out of conformance.

Through testing, the value of 1 second will be validated or updated in future versions of this document tbd_timeconform. This requirement may be achieved through:

- regular position reporting,
- a messaging system between the USS and operators,
- some other means.

[UTM-USS-047] The USS MUST maintain a record of the state of a nonconforming operation as NONCONFORMING.

Note that some ways of entering the NONCONFORMING state will not be immediately knowable by the USS (weather limits, visibility conditions, etc.). There may be future requirements on how aware a USS needs to be aware of such operational elements tbd_conformawareness.

[UTM-USS-048] A USS MUST announce to its LUN a NONCONFORMING operation within 2 seconds of transitioning an operation into the NONCONFORMING state.

[UTM-USS-049] A USS MUST announce to its LUN within 2 seconds of transitioning an operation into the ACTIVATED state from the NONCONFORMING state.

[UTM-USS-050] A USS MUST designate the state of an operation that has been in the NONCONFORMING state for 30 continuous seconds as ROGUE.

[UTM-USS-051] A USS MUST designate the state of an operation that has transitioned to the NONCONFORMING 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.

[UTM-USS-052] A USS MUST designate the state of an operation that is not contained within at least one of its Operation Volumes as ROGUE.

This requirement emphasizes the importance of an operator staying within its Conformance Volumes, and failing that, ensuring the operation does not breach the collection of Operation Volumes.

[UTM-USS-053] A USS MUST announce to its LUN a ROGUE operation within 2 seconds of transitioning that operation to the ROGUE state.

A USS may transition an operation to the ACTIVATED or CLOSED states from the NONCONFORMING state when the operation meets the requirements of those state definitions.

[UTM-USS-054] A USS MUST NOT transition a ROGUE operation to any state other than CLOSED.

[UTM-USS-055] 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 requirements implies that a ROGUE operation has no option other than to become CLOSED (see Figure 2). A ROGUE operation may instigate reactions from other stakeholders on the ground and in the air. It is not reasonable to allow such an operation to return to a nominal state given the potential side effects of that operation becoming ROGUE.

There is one important follow-up note regarding the definition of a Conformance Volume. Given that Part 107 and hobbyist operations are not required to report positions to the USS, it may be challenging to know when or if such an operation becomes NONCONFORMING. It might be that the Conformance Volumes are equal to the Operation Volumes (geographically speaking). In this case, an operation could not become NONCONFORMING due to a volume-related violation; it would immediately become ROGUE if it left its Conformance/Operation Volume. This concept should be carefully considered by the USS when determining how it supports its operators and how that support is explained to its operators.

9.3. Contingency Management

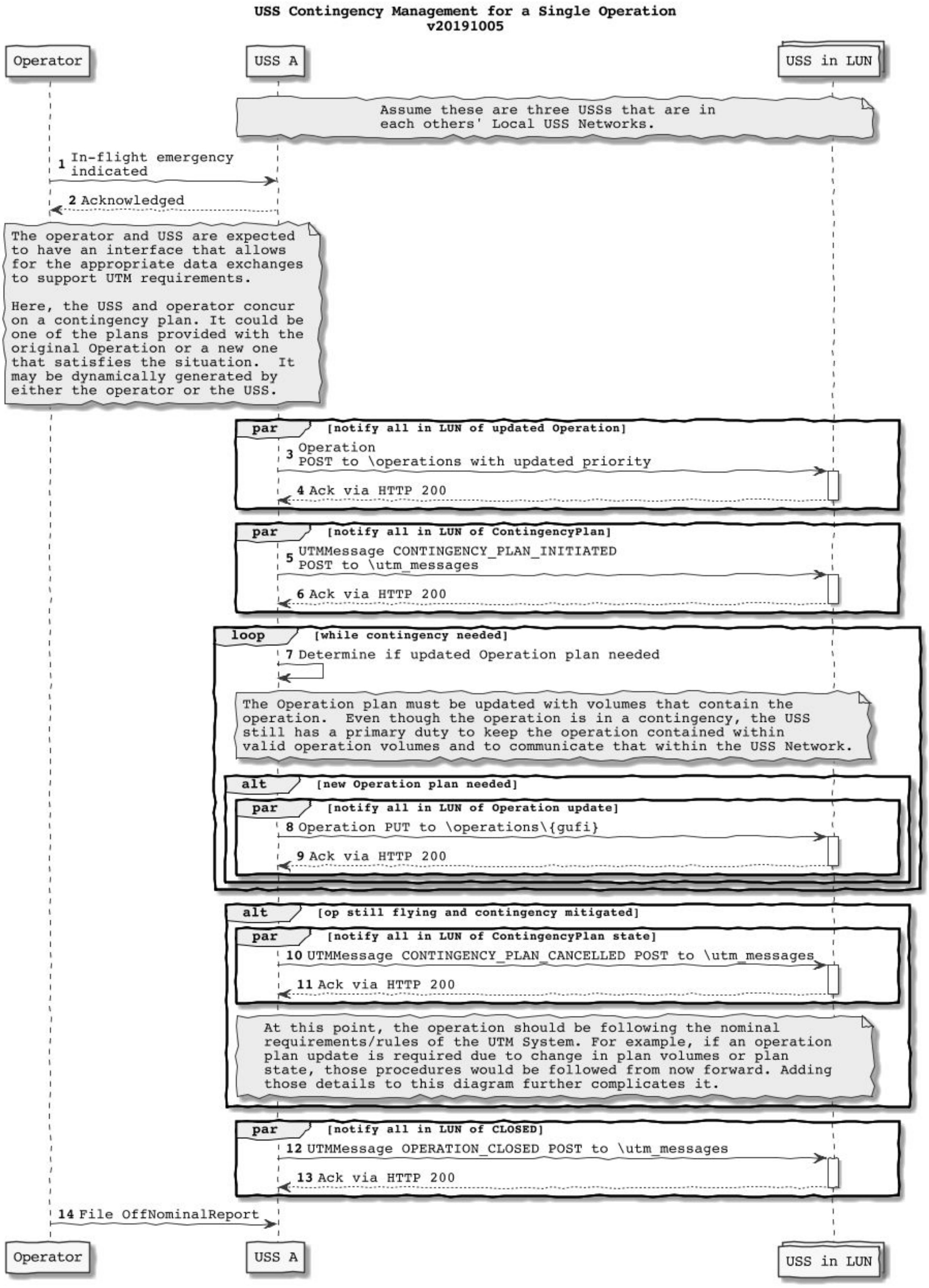
Per the [USSREQ-API], an Operation contains a set of Contingency Plans. The Contingency Plan provides a preflight method to communicate how various unplanned situations might be handled by an operation. Each plan lists a non-empty set of events or conditions, each with a single contingency response.

[UTM-USS-056] A USS MUST provide at least one Contingency Plan per Operation Volume within an Operation plan as defined per the [USSREQ-API].

[UTM-USS-057] When a Contingency Plan is put into action, the USS MUST post a message containing the Contingency Plan to each USS in its LUN.

[UTM-USS-058] A USS MUST update the LUN via a 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. The following sequence diagram (Figure 4) is informative of the expected communications between stakeholders:


USS Contingency Management for a Single Operation
v20191005
Operator
USS A
USS in LUN
par
[notify all in LUN of updated Operation]
par
[notify all in LUN of ContingencyPlan]
loop
[while contingency needed]
alt
[new Operation plan needed]
par
[notify all in LUN of Operation update]
alt
[op still flying and contingency mitigated]
par
[notify all in LUN of ContingencyPlan state]
par
[notify all in LUN of CLOSED]
Operator
USS A
USS in LUN

Assume these are three USSs that are in each others' Local USS Networks.

1 In-flight emergency indicated

2 Acknowledged

The operator and USS are expected to have an interface that allows for the appropriate data exchanges to support UTM requirements.

Here, the USS and operator concur on a contingency plan. It could be one of the plans provided with the original Operation or a new one that satisfies the situation. It may be dynamically generated by either the operator or the USS.

3 Operation POST to \operations with updated priority

4 Ack via HTTP 200

5 UTMMessage CONTINGENCY_PLAN_INITIATED POST to \utm_messages

6 Ack via HTTP 200

7 Determine if updated Operation plan needed

The Operation plan must be updated with volumes that contain the operation. Even though the operation is in a contingency, the USS still has a primary duty to keep the operation contained within valid operation volumes and to communicate that within the USS Network.

8 Operation PUT to \operations\{gufi}

9 Ack via HTTP 200

10 UTMMessage CONTINGENCY_PLAN_CANCELLED POST to \utm_messages

11 Ack via HTTP 200

At this point, the operation should be following the nominal requirements/rules of the UTM System. For example, if an operation plan update is required due to change in plan volumes or plan state, those procedures would be followed from now forward. Adding those details to this diagram further complicates it.

12 UTMMessage OPERATION_CLOSED POST to \utm_messages

13 Ack via HTTP 200

14 File OffNominalReport

Figure 4. Contingency Management for a Single Operation.

10. UAS Volume Reservations

A UAS Volume Reservation (UVR) is a 4-dimensional volume with additional properties that affect UAS operations by limiting access to that 4-dimensional volume. Currently, the [USSREQ-API] defines an endpoint for new UVRs to be posted to a USS. These could be constraints that are generated by some other entity in the NAS that are communicated via FIMS or constraints that are generated by another USS with the appropriate role. Thus USSs that are currently active will receive data regarding UVRs that may affect their supported operations. The entity that provides the original announcement for a UVR will be available to query for UVR details. This is useful for USSs that come online or become active in a new geographic region after the initial UVR announcement. The USS Discovery document or future FAA or NASA concept documents may provide additional insight or requirements in regard to UVRs, thus beyond the references to UVRs in the [USSREQ-API], the concept and requirements will be deferred to those future documents[tbd_uvrs]. The FAA-NASA UTM Pilot Program tested the concept of UVRs, and results from that testing will likely inform future requirements.

11. Priority Operations

Certain UAS operations in the UTM airspace may be designated as priority operations. Operations that are not priority operations are designated as nominal operations. Currently, there are two types of priority operation: emergencies and public safety. Priority operations have a severity level assigned to them. These levels are defined in the APIs and allow for ranking of priority operations. There is no difference in ranking inherently between emergencies and public safety operations; they are only differentiated (in terms of conflict management) by their assigned severity levels. A priority operation is of higher priority than each nominal operation. One priority operation is of higher priority if its severity level is higher.

The two types of priority operations are described in the subsections below. An operation of higher priority will force a change in the operational plans of lower priority when their plans intersect.

[UTM-USS-059] A USS MUST define and announce an updated, deconflicted operation plan for an operation that intersects another operation of higher priority within 30 seconds of the announcement of the higher priority operation.

See Negotiation section for more information.

11.1. In-flight Emergency

Any USS can designate an operation under its management as being in an in-flight emergency state. Note that this state is separate from the regular operation state discussed above. An operation can be in the ACTIVATED, NONCONFORMING, or

ROGUE states and also be in or out of an in-flight emergency state. Until there are more specific definitions of an in-flight emergency for sUAS, UTM refers to the NAS definition of an in-flight emergency for manned aviation: An in-flight emergency is a distress or urgency condition. The [FAAGlossary] defines an urgency condition as "being concerned about safety and of requiring timely but not immediate assistance; a potential distress condition" while a distress is defined as "a condition of being threatened by serious and/or imminent danger and of requiring immediate assistance." Typically the pilot in command (PIC), or RPIC in UTM's case, makes this determination. In UTM, the USS may make this determination on the RPIC's behalf. If the RPIC or the USS determines an operation is in an in-flight emergency (distress or urgency condition), the USS will need to notify appropriate stakeholders.

[UTM-USS-060] A USS MUST send a message to its LUN when an in-flight emergency is determined for an operation under its management.

[UTM-USS-061] A message describing an operation in an urgency condition MUST denote a severity level lower than EMERGENCY according to the UTM API documentation.

[UTM-USS-062] A message describing an operation in a distress condition MUST denote a severity level of EMERGENCY.

[UTM-USS-063] A USS MUST update the operation plan of an operation under its management that enters or exits an in-flight emergency state.

This update will include an appropriate setting of the priority elements based on the type of in-flight emergency and will update the operation volumes to accommodate the emergency, if necessary. A USS should ensure that an operation does not enter the NONCONFORMING or ROGUE states while handling an in-flight emergency.

A useful reference for off-nominal situations from the operator perspective is [UTM-OffNominal]. Additional requirements and discussion for off-nominal operations are provided in the Accounting and Auditing section below.

11.2. Public Safety

A USS may complete additional checkout steps to earn a public safety USS role. These steps are TBD, however they may include higher levels of QoS, documentation of a process to vet and handle public safety personnel, and additional assurances of ethical behavior in the UTM airspace, amongst other requirements.

Upon earning the public safety role, a USS may then accept public safety operations from public safety operators (e.g., police, firefighting, emergency medical services). Public safety operations have a higher priority than regular operations. However, note that not all operations submitted by a public safety operator are priority operations. In other words, a public safety operator may choose to submit regular operations as well as public safety operations.

12. USS-USS Communication

Collaboration is a key feature of the UTM System. To successfully collaborate, the communication between USSs is described here.

The [USSREQ-API] standardizes the expectations of the communication mechanisms to be provided by each USS such as the endpoints and the data models. This section helps describe more requirements on HOW to use the API.

12.1. Operation Announcements

[UTM-USS-064] A USS MUST announce a new Operation via the [USSREQ-API] to all USSs that intersect that new Operation.

Currently, this is achieved via an HTTP POST to the "/operations" endpoint of each of those intersecting USSs, though this document defers to the current [USSREQ-API] for the correct mechanism.

[UTM-USS-065] A USS MUST announce modifications to an existing Operation via the [USSREQ-API] to all USS Instances that intersect the modified Operation.

This requirement has several implications that an implementer needs to consider. First, the modification announcement might go to a USS that was not required to receive the initial announcement of that operation. Thus, if this is handled with an HTTP PUT to the "/operations" endpoint, that new USS would not necessarily have data to be modified by the PUT.

Depending from which state the Operation transitions to CLOSED, there are specific severity levels that are required and described in the [USSREQ-API] and are not reprinted here to reduce potential documentation conflicts.

12.2. Position Reports

[UTM-USS-066] A USS MUST collect position updates from all ACTIVATED Part 107X operations that it manages.

[UTM-USS-067] A USS MUST provide access to all Part 107X operation position updates from operations that it manages to FIMS upon request per the [USSREQ-API].

[UTM-USS-068] A USS MUST provide access to position updates for a Part 107X operation that it manages (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.

If you have an operation crossing another USS's operation, you need to exchange position data with each other upon request. This document defers to [USSREQ-API] on how this is achieved. Currently this is achieved by a requesting USS to send a message to another USS to "turn on" or "turn off" position reporting for a particular operation. Positions are provided as HTTP PUTs to the requesting USS at a frequency of 1Hz. Note that if the negotiation process described in the next section results in strategic deconfliction of the operations, there will be no intersection operation volumes from two separate operations.

[UTM-USS-069] A USS MUST provide access to position updates (if available) for operations that it manages to its LUN for all operations in the ROGUE or NONCONFORMING states.

12.3. Strategic Deconfliction

Details and discussion of this section are deferred to [UTM-SD]. The requirements from that reference are supplied here for completeness.

- A UTM Operation should be free of 4-D intersection with all other known UTM Operations prior to departure and this should be known as "Strategic Deconfliction" within UTM. The Strategic Deconfliction scheme:
    - *[UTM-CM.05] MUST have the 4-D non-intersection of operations as its primary objective.*
    - *[UTM-CM.10] MUST be well-documented for the understanding of operators.*
    - *[UTM-CM.12] MUST allow for inspection of decisions by operators upon request from operators to their supporting USS.*
    - *[UTM-CM.15] MUST be supported by all USSs*
    - *[UTM-CM.20] MUST be mandated by the airspace regulator.*
- Strategic Deconfliction needs a prioritization scheme for operations within UTM. The Prioritization scheme:
    - *[UTM-CM.25] MUST allow for preemption of operations with lower priority by those with higher priority.*
    - *[UTM-CM.30] MUST be equivalently calculable by each USS given the same operation data.*
    - *[UTM-CM.35] MUST be efficiently calculable by each USS given the same operation data.*
    - *[UTM-CM.37] MUST be independently calculable by USSs given the same operation data.*
    - [UTM-CM.40] SHOULD be a function of operator, operation, airspace, and vehicle parameters.
- Strategic Deconfliction needs an allowance for negotiating deconfliction of UTM operations. The Negotiation scheme:
    - *[UTM-CM.45] MUST minimize direct human interaction.*
    - *[UTM-CM.50] MUST be facilitated via USSs.*
    - *[UTM-CM.55] MUST be a finite process.*
- Strategic Deconfliction needs an allowance for intersecting UTM operations. Intersecting operators, via their USSs:
    - *[UTM-CM.60] MUST have preceded the decision to intersect with a negotiation process.*

- ○ *[UTM-CM.65] MUST each provide explicit acknowledgement to each other of the planned intersection of operation volumes when intersection is mutually decided.*
- ○ *[UTM-CM.70] MUST each provide details to each other on the approach to a separation provision while in intersecting operation volumes when intersection is mutually decided.*

APIs to support Strategic Deconfliction, including negotiation, are part of the [USSREQ-API].

12.4. Information Sharing

There might be future requirements for airspace information sharing between operators. The first approach will use a system as roughly described in [UREP] for sharing what are being called "UAS Reports." As a placeholder for future discussions[tbd_urep] on this topic, the following requirements are provided:

[UTM-USS-070] A USS MUST offer a method for operators with operations under that USS's management to report weather and air traffic observations.

[UTM-USS-071] A USS MUST share reports regarding weather and air traffic as supplied by an operator, with other UTM stakeholders.

[UTM-USS-072] A USS MUST provide a means for operators with operations under that USS's management to receive weather and air traffic observations from other stakeholders.

To satisfy these requirements initially and in an interoperable way, a USS SHOULD use the [UREP-API]. In future versions of this document, pending discussions, that last statement may become a requirement and likely will be a requirement for USS checkout purposes.

13. 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.

[UTM-USS-073] Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a digital signature of the most recent version of an operation plan by the RPIC for that operation.

[UTM-USS-074] Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a digital signature of the most recent version of an operation plan by the vehicle for that operation.

[UTM-USS-075] Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a copy of all operation authorizations, if any, under which that operation will be performed.

The signing of an operation plan by a vehicle and an RPIC provides assurance that the resources noted within the operation 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 a 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 transitioned to the ACCEPTED state before signing takes place as this allows for some last minute alterations in the involved parties to support a variety of use cases. The method for signing by RPICs and vehicles has not yet been determined[tbd_sign].

A USS will have requirements for storing logs of queries and connections to its systems. Requirements for formats and duration of archives will be determined in the future and will be updated in this specification[tbd_logging].

When an operation enters an off-nominal condition (which would include all NONCONFORMING and ROGUE operations), additional reporting will be necessary. For more discussion and definitions for off-nominal conditions, see [UTM-OffNominal].

[UTM-USS-076] A USS MUST obtain an off-nominal situation report from the operator for each ROGUE operation.

[UTM-USS-077] A USS MUST obtain an off-nominal situation report from the operator for each operation that has an unplanned return to the launch location.

[UTM-USS-078] A USS MUST obtain an off-nominal situation report from the operator for each operation that has an unplanned landing.

[UTM-USS-079] A USS MUST obtain an off-nominal situation report from the operator for each operation that enters an unplanned loiter.

The definition of “unplanned” in the previous requirements relates to the active operation plan at the time of the landing or at the time of the loiter. It is quite possible in these cases that the operation goes ROGUE in the process of such a landing or loiter, but this is not necessarily the case. Thus, the separate requirements are needed.

The separate requirements for unplanned landing ([UTM-USS-078]) and unplanned return to launch location ([UTM-USS-077]) stem from the way in which those landings may occur. For example manual versus automated or controlled versus uncontrolled. Through further discussion with stakeholders, these requirements may be refined and potentially collapsed or further expanded [tbd_landing].

[UTM-USS-080] A USS MUST obtain an off-nominal situation report from the operator for each operation results in the loss of the UA.

The “loss of the UA” means either

- a total loss of the vehicle due to a crash or hard landing, or
- a vehicle that is unrecoverable due to its known or unknown landing location.

[UTM-USS-081] Whenever a USS is required to obtain an off-nominal situation report from an operator, the USS MUST do so within 3 days of the operation completion.

[UTM-USS-082] A USS MUST obtain data from the operator's platform per a Data Management Plan.

Formatting of off-nominal situation reports will be codified in the future and may allow for reporting multiple events in a single form, but currently the expectation is that for each requirement that is met above for an operation, there will be a unique off-nominal situation. So an operation that goes NONCONFORMING twice would submit two reports. An operation that suddenly loiters and then later in the operation goes NONCONFORMING would need to file two off-nominal situation reports. Again, this process will be developed further in the future to streamline as much as possible without losing potentially vital airspace safety information.

Data management plan details will be published in a separate document in the future [tbd_dmp].

14. 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 QoS that need to be maintained by each USS Instance. This section captures those QoS elements not captured elsewhere in this document. The QoS measures and metrics will be defined in a future version of this document[tbd_qos]. Possible examples of QoS metrics include:

1. Nonconforming 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)
4. Message response latency
5. Successful negotiations
6. Intersecting volumes minimized
7. Data quality metrics

15. 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.

16. 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 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 this writing).
4. Apply for checkout process.
5. Software checkout.
6. Obtain identity information from ANSP/FIMS.

Further detail or formalization is currently beyond the scope of this document. For some further insight on some of these steps, see [USSCheckout].

Step 6 above will follow [NIST800.63.3] Digital Identity Guidelines. USS identities in the UTM System will be assured according to the following levels in [NIST800.63.3]:

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 [NIST800.63.3]. 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. A separate document (or set of documents) will further detail the USS identity assurance system within UTM[tbd_id].

17. Threat Modeling

Many of the requirements in this document were driven by various threat modeling exercises. Separate documentation may be produced in the future providing summaries of those threat modeling exercises.

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>.
[RFC3629]	Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.
[RFC4086]	Eastlake 3rd, D.,Schiller, J., Crocker, S., "Randomness Requirements for Security," RFC 4086, DOI: 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.
[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>.
[RFC6819]	Lodderstedt, T., McGloin M., Hunt, P., "OAuth 2.0 Threat Model and Security Considerations", RFC 6819, DOI: 10.17487/RFC6819, January 2013, <https://www.rfc-editor.org/info/rfc6819>.
[RFC7231]	R. Fielding, R., Ed., Reschke, J., Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI: 10.17487/RFC7231, June 2104, <https://www.rfc-editor.org/info/rfc7231>.
[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 >.
[RFC7800]	Jones M., Bradley J., Tschofenig H., "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, DOI: 10.17487/RFC7800, April 2016, <https://www.rfc-editor.org/info/rfc7800>.
[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>.
[RFC8259]	Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", December 2017, <https://www.rfc-editor.org/info/rfc8259>.
National Institute of Standards and Technology Documents	

[NIST800.52.2]	Barker, E., "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (2nd Draft)", NIST Special Publication 800-52 Revision 2 Draft, October 2018, <https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf>.
[NIST800.57.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>.
[NIST800.57.p2]	Barker, E., et al., "Recommendation for Key Management – Part 2: Best Practices for Key Management Organization", NIST Special Publication 800-57 Part 2, <http://dx.doi.org/10.6028/NIST.SP.800-57p2>.
[NIST800.57.p3]	Barker, E., Dang, Q., "Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance", NIST Special Publication 800-57 Part 3 Revision 1, January 2015, <http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1>.
[NIST800.63.3]	NIST, "Digital Identity Guidelines", <https://pages.nist.gov/800-63-3/>.
[NIST800.90A.R1]	Barker, E., Kelsey, J., "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", NIST Special Publication 800-90A Revision 1, June 2015, <http://dx.doi.org/10.6028/NIST.SP.800-90Ar1>.
[NIST800.90A.R1.LIST]	NIST, "DRBG Validation List", <http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html>.
[NIST800.122]	NIST, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.
UTM Application Programming Interface Specifications	
[USSDS-API]	https://github.com/interuss/dss
[FIMSAuthzAPI]	https://github.com/nasa/utm-apis/tree/v4-draft/fimsauthz-api
[FIMSUSS-API]	https://github.com/nasa/utm-apis/tree/v4-draft/fims-api
[USSREQ-API]	https://github.com/nasa/utm-apis/tree/v4-draft/uss-api
[PUBSAFE-API]	https://github.com/nasa/utm-apis/tree/v4-draft/public-safety-uss
[UREP-API]	https://github.com/nasa/utm-apis/tree/v4-draft/urep-api
FAA	
[FAAConOps]	FAA NextGen Office, "Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations", v1.0, May 2018.
[FAAGlossary]	FAA Pilot/Controller Glossary, <https://www.faa.gov/air_traffic/publications/media/pcg.pdf>.
[FAA107]	Part 107–Small Unmanned Aircraft Systems, <https://www.ecfr.gov/cgi-bin/text-idx?node=pt14.2.107>
NASA	
[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>.*
[UTMAuth]	*Rios, J., Smith, I., Venkatesan, P., "UTM Authentication and Authorization Framework", NASA TM-2019-220364, September 2019.*
[NASAConOps]	*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.*
[UREP]	*Rios, J., Smith, D., Smith, I., "UAS Reports (UREPs): Enabling Exchange of Observation Data Between UAS Operations", NASA TM-2017-219462, February 2017.*
[USSCheckout]	*Smith, I.,Rios,J.,Mulfinger, D.,Baskaran,V.,Verma, P., "USS Checkout: How UTM Confirmed Readiness of Flight Tests with UAS Service Suppliers", NASA Technical Memo planned for December 2019.*
[UTM-SD]	*Rios, J., "Strategic Deconfliction: System Requirements, Final Report". 31 Jul 2018, accessed 11-Oct-2019, <https://utm.arc.nasa.gov/docs/2018-UTM-Strategic-Deconfliction-Final-Report.pdf>.*
[UTM-OffNominal]	*Jung, J., “Communications and Navigation Off-Nominal Situations Management: Concept of Operations & Requirements,” NASA, 17 May 2018.*
Other Documents	
[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-Jul-2017, <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>.*
[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>.*
*[JW*Blog]*	*Siriwardena, P., "JWT, JWS and JWE for Not So Dummies!", Blog post, retrieved 31 Aug 2017, written 26 Apr 2016, <https://medium.facilelogin.com/jwt-jws-and-jwe-for-not-so-dummies-b63310d201a3>.*
[HTTPSign]	*https://tools.ietf.org/html/draft-cavage-http-signatures-07 .*
[AmzSign]	*http://docs.aws.amazon.com/AmazonS3/latest/dev/RESTAuthentication.html .*

[UTMDisc]	*“InterUSS Platform,” InterUSS Project, Linux Foundation, accessed 11-Oct-2019, https://interussplatform.org.*
[InterUSS]	*“InterUSS Platform,”*

Elements for Future Research and Definition

Tag in text	Description
tbd_alt	*Determine additional requirements related to altitude reporting and transformation.*
tbd_time	*Determine appropriate time synchronization approach for USSs and FIMS.*
tbd_logging	*Determine requirements for logging data including formats, content, and duration of archiving.*
tbd_vols	*Determine requirements/limits on the definitions of 4D volumes, including how many, lateral size, longitudinal size, max height, max duration, and/or overall 4D volume measurement.*
tbd_timeconform	*Determine requirements on how soon a USS must know about an operation leaving conformance/entering NONCONFORMING state.*
tbd_conformawareness	*Determine requirements for how aware a USS must be in terms of non-position/time elements of an operation that determine its conformance. For example, visibility, surveillance coverage, C2 conditions, etc.*
tbd_uvrs	*Determine requirements related to supporting UAS Volume Reservations.*
tbd_urep	*Determine the required mechanisms for operator-operator information sharing.*
tbd_sign	*Determine the approach to signing operation plans by the vehicle and RPIC.*
tbd_landing	*Determine appropriate reporting requirements for various types of off-nominal landings.*
tbd_dmp	*Determine the data management plan for data not typically part of USS-FIMS or USS-USS communications. Example is off-nominal reporting forms/data.*
tbd_qos	*Determine quality of service requirements for a USS, including elements such as up time, response latency, etc.*
tbd_id	*Determine requirements or guidelines for identity management for a USS.*

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 and title.

Req. ID	Requirement
[UTM-USS-001]	A USS MUST meet the requirements of the authorizing entity for authority to operate as a USS.
[UTM-USS-002]	All data exchanges via UTM APIs MUST be completed over a TLS-secured connection.
[UTM-USS-003]	All TLS implementations for UTM data exchanges MUST conform to the most recent version of NIST 800-52.
[UTM-USS-004]	A USS MUST communicate with FIMS per the [FIMSUSS-API] and the [USSREQ-API].
[UTM-USS-005]	A USS MUST communicate with other USSs per the [USSREQ-API].
[UTM-USS-006]	A USS MUST use the [FIMSAuthzAPI] for authorization purposes with other USSs.
[UTM-USS-007]	A USS MUST use the [FIMSAuthzAPI] for authorization purposes with FIMS.
[UTM-USS-008]	A USS MUST implement the [PUBSAFEAPI].
[UTM-USS-009]	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-010]	When generating a UUID, a USS MUST generate a version 4 UUID as per [RFC4122].
[UTM-USS-011]	JSON text exchanged between USSs MUST be encoded using UTF-8.
[UTM-USS-012]	JSON text exchanged between a USS and FIMS MUST be encoded using UTF-8.
[UTM-USS-013]	A USS MUST treat the presence of a byte order mark as a malformed data exchange.
[UTM-USS-014]	For any exchange of JSON-formatted data, the receiver MUST reply with an HTTP 400 status code whenever any required field (as specified in the relevant schema definition) of the received data is missing.
[UTM-USS-015]	If malformed data are received via a RESTful call, the receiver MUST reply with an HTTP 400 status code.
[UTM-USS-016]	A USS MUST NOT reject JSON due to the ordering of fields within the JSON.
[UTM-USS-017]	A USS MUST adhere to API specifications related to units of measure and their formatting.
[UTM-USS-018]	A USS MUST use UTC time for all date-times exchanged with other USSs.
[UTM-USS-019]	A USS MUST use UTC time for all date-times exchanged with FIMS.
[UTM-USS-020]	All date-times supplied by a USS to another USS MUST follow the format pattern YYYY-MM-DDThh:mm:ss.sssZ.
[UTM-USS-021]	All date-times supplied by a USS to FIMS MUST follow the format pattern YYYY-MM-DDThh:mm:ss.sssZ.
[UTM-USS-022]	A USS MUST verify that time strings have the format YYYY-MM-DDThh:mm:ss.sssZ.

[UTM-USS-023]	All altitudes within UTM MUST be in reference to World Geodetic System 1984 [WGS 84].
[UTM-USS-024]	To convert between feet and meters, the USS MUST use a factor of 0.3048 m/ft.
[UTM-USS-025]	A USS MUST adhere to the requirements described in [UTMAuth].
[UTM-USS-026]	A USS MUST NOT request tokens with duplicate parameters while it is in possession of a valid token with those parameters and a valid use time of at least 50% of its initial valid use time.
[UTM-USS-027]	A USS MUST ensure that its access tokens stored on its systems are inaccessible to external entities.
[UTM-USS-028]	A USS MUST remove all traces of another USS's valid access token from its systems after the token serves its purpose of authorizing appropriate access.
[UTM-USS-029]	A USS MUST adhere to the requirements for discovery as described in [UTMDisc].
[UTM-USS-030]	A USS MUST protect an operator's Personally Identifiable Information (PII) from unlawful and/or unintended disclosure.
[UTM-USS-031]	Prior to a non-hobbyist operation, a USS MUST ensure the vehicle designated for an Operation it is supporting is properly registered.
[UTM-USS-032]	A USS MUST ensure that a UAS operator's plan conforms to published airspace rules and regulations.
[UTM-USS-033]	A USS MUST supply a position report from within the last 2 seconds for any non-hobbyist operation supported by that USS within 1 second of receiving an authorized request for that position.
[UTM-USS-034]	When requested, a USS MUST supply operation information to the requesting operator associated with that operation.
[UTM-USS-035]	A USS MUST offer a mechanism to receive messages related to in-flight emergencies from a supported operation.
[UTM-USS-036]	A USS MUST acknowledge a message related to an in-flight emergency from a supported operation.
[UTM-USS-037]	A USS MUST assign a GUFI as a UUIDv4 for each supported operation.
[UTM-USS-038]	A USS MUST keep a GUFI constant once assigned to an operation.
[UTM-USS-039]	A USS MUST report the valid state of an operation within 2 seconds of receiving a valid request for that state.
[UTM-USS-040]	A USS MUST maintain the state of an operation as ACCEPTED at all times from announcing it via the UTM APIs until an event causes a transition to another state.
[UTM-USS-041]	A USS MUST maintain the state of an operation as ACTIVATED at all times after the start time of its first operation volume until it is closed while it is in conformance with its plan and the rules of the airspace.
[UTM-USS-042]	A USS MUST transition an operation to the CLOSED state when it is no longer flying and will not fly again.
[UTM-USS-043]	A USS MUST announce any transition to the CLOSED state to its LUN.
[UTM-USS-044]	A USS MUST define a Conformance Volume for each Operation Volume for each operation.
[UTM-USS-045]	A Conformance Volume MUST be contained in all four dimensions within its associated Operation Volume.
[UTM-USS-046]	A USS MUST be aware within 1 second that an operation under its management is

	out of conformance.
[UTM-USS-047]	The USS MUST maintain a record of the state of a nonconforming operation as NONCONFORMING.
[UTM-USS-048]	A USS MUST announce to its LUN a NONCONFORMING operation within 2 seconds of transitioning an operation into the NONCONFORMING state.
[UTM-USS-049]	A USS MUST announce to its LUN within 2 seconds of transitioning an operation into the ACTIVATED state from the NONCONFORMING state.
[UTM-USS-050]	A USS MUST designate the state of an operation that has been in the NONCONFORMING state for 30 continuous seconds as ROGUE.
[UTM-USS-051]	A USS MUST designate the state of an operation that has transitioned to the NONCONFORMING state more than 3 times as ROGUE.
[UTM-USS-052]	A USS MUST designate the state of an operation that is not contained within at least one of its Operation Volumes as ROGUE.
[UTM-USS-053]	A USS MUST announce to its LUN a ROGUE operation within 2 seconds of transitioning that operation to the ROGUE state.
[UTM-USS-054]	A USS MUST NOT transition a ROGUE operation to any state other than CLOSED.
[UTM-USS-055]	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.
[UTM-USS-056]	A USS MUST provide at least one Contingency Plan per Operation Volume within an Operation plan as defined per the [USSREQ-API].
[UTM-USS-057]	When a Contingency Plan is put into action, the USS MUST post a message containing the Contingency Plan to each USS in its LUN.
[UTM-USS-058]	A USS MUST update the LUN via a message when any Contingency Plan ends or changes.
[UTM-USS-059]	A USS MUST define and announce an updated, deconflicted operation plan for an operation that intersects another operation of higher priority within 30 seconds of the announcement of the higher priority operation.
[UTM-USS-060]	A USS MUST send a message to its LUN when an in-flight emergency is determined for an operation under its management.
[UTM-USS-061]	A message describing an operation in an urgency condition MUST denote a severity level lower than EMERGENCY according to the UTM API documentation.
[UTM-USS-062]	A message describing an operation in a distress condition MUST denote a severity level of EMERGENCY.
[UTM-USS-063]	A USS MUST update the operation plan of an operation under its management that enters or exits an in-flight emergency state.
[UTM-USS-064]	A USS MUST announce a new Operation via the [USSREQ-API] to all USSs that intersect that new Operation.
[UTM-USS-065]	A USS MUST announce modifications to an existing Operation via the [USSREQ-API] to all USS Instances that intersect the modified Operation.
[UTM-USS-066]	A USS MUST collect position updates from all ACTIVATED Part 107X operations that it manages.
[UTM-USS-067]	A USS MUST provide access to all Part 107X operation position updates from operations that it manages to FIMS upon request per the [USSREQ-API].
[UTM-USS-068]	A USS MUST provide access to position updates for a Part 107X operation that it manages (Operation A) to another USS upon request when that second USS has an

	active operation with an operation volume intersecting Operation
[UTM-USS-069]	A USS MUST provide access to position updates (if available) for operations that it manages to its LUN for all operations in the ROGUE or NONCONFORMING states.
[UTM-USS-070]	A USS MUST offer a method for operators with operations under that USS's management to report weather and air traffic observations.
[UTM-USS-071]	A USS MUST share reports regarding weather and air traffic as supplied by an operator, with other UTM stakeholders.
[UTM-USS-072]	A USS MUST provide a means for operators with operations under that USS's management to receive weather and air traffic observations from other stakeholders.
[UTM-USS-073]	Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a digital signature of the most recent version of an operation plan by the RPIC for that operation.
[UTM-USS-074]	Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a digital signature of the most recent version of an operation plan by the vehicle for that operation.
[UTM-USS-075]	Prior to a non-hobbyist operation becoming ACTIVATED, a USS MUST obtain a copy of all operation authorizations, if any, under which that operation will be performed.
[UTM-USS-076]	A USS MUST obtain an off-nominal situation report from the operator for each ROGUE operation.
[UTM-USS-077]	A USS MUST obtain an off-nominal situation report from the operator for each operation that has an unplanned return to the launch location.
[UTM-USS-078]	A USS MUST obtain an off-nominal situation report from the operator for each operation that has an unplanned landing.
[UTM-USS-079]	A USS MUST obtain an off-nominal situation report from the operator for each operation that enters an unplanned loiter.
[UTM-USS-080]	A USS MUST obtain an off-nominal situation report from the operator for each operation results in the loss of the UA.
[UTM-USS-081]	Whenever a USS is required to obtain an off-nominal situation report from an operator, the USS MUST do so within 3 days of the operation completion.
[UTM-USS-082]	A USS MUST obtain data from the operator's platform per a Data Management Plan.