DRIP
Internet-Draft
Intended status: Informational
Expires: 23 October 2020

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao
Tencent
21 April 2020

Drone Remote Identification Protocol (DRIP) Architecture
draft-card-drip-arch-02

Abstract

This document defines an architecture for Drone Remote Identification Protocol (DRIP) Working Group protocols and services to support Unmanned Aircraft System Remote Identification (UAS RID) and RID-related communications, including its building blocks and their interfaces, all to be standardized.

CAVEAT LECTOR: This draft version is undergoing substantial restructuring and is submitted to the DRIP WG only to spark discussion on architecture and to be adopted as a placeholder if there is consensus that there should be an architecture document (however far from any future consensus on that architecture this draft may be).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 October 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
1.1. UAS RID Uses 4
1.2. UAS RID Design Considerations 5
1.3. DRIP Goals 5
2. Terms and Definitions 5
2.1. Requirements Terminology 6
2.2. Additional Definitions 6
3. Entities and their Interfaces 7
3.1. Private Information Registry 7
3.1.1. Background 7
3.1.2. Proposed Approach 7
3.2. Public Information Registry 8
3.2.1. Background 8
3.2.2. Proposed Approach 8
3.3. CS-RID concept 8
3.3.1. Proposed optional CS-RID SDSP 8
3.3.2. Proposed optional CS-RID Finder 9
4. Identifiers 9
4.1. Background 9
4.2. Proposed Approach 10
5. Proposed Transactions 10
6. IANA Considerations 11
7. Security Considerations 11
8. Acknowledgments 11
9. References 11
9.1. Normative References 11
9.2. Informative References 12

Appendix A. Overview of Unmanned Aircraft Systems (UAS) Traffic Management (UTM) 14
A.1. Operation Concept 14
A.2. UAS service supplier (USS) 14
A.3. UTM Use cases for UAS operation 15

A.4. Overview UAS Remote ID (RID) and RID Standardization . . 15
Authors' Addresses 16

1. Introduction

Many safety and other considerations dictate that Unmanned Aircraft (UA) be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating Unmanned Aircraft Systems (UAS) Remote Identification (RID). The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The United States Federal Aviation Administration (FAA) has published a Notice of Proposed Rule Making [NPRM]. CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed the new ASTM [F3411-19] Standard Specification for Remote ID and Tracking. It defines 1 set of RID information and 2 means of communicating it (if a UAS uses both communication methods, the CAAs are expected to mandate that the RID information content will be identical over both methods).

> Network RID defines a RID data dictionary and data flow: from a UAS via unspecified means to a Network Remote ID Service Provider (Net-RID SP); from the Net-RID SP to an integrated, or over the Internet to a separate, Network Remote ID Display Provider (Net-RID DP); from the Net-RID DP via the Internet to Network Remote ID clients in response to their queries (expected typically, but not specified exclusively, to be web based) specifying airspace volumes of interest. Network RID depends upon connectivity, in several segments, including the Internet, from the UAS to the Observer.
>
> Broadcast RID defines a set of RID messages and how the UA

transmits them locally directly one-way, over Bluetooth or Wi-Fi. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the locally directly received UAS ID as a key. Broadcast RID should be functionally usable in situations with no Internet connectivity.

Other SDOs (e.g. 3GPP, Appendix A.4) may define their own communication methods for both Network and Broadcast RID. The CAAs expect any additional methods to maintain consistency of the RID messages.

[F3411-19] specifies 3 UAS ID Types.

1. 1: a static, manufacturer assigned, hardware serial number per ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A].

2. 2: a CAA assigned (presumably static) ID.

3. 3: a UAS Traffic Management (UTM) system assigned UUID v4 [RFC4122], which can but need not be dynamic.

The EU allows only Type 1. The US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once (for a single UAS flight, which in the context of UTM is called an "operation"). [F3411-19] Broadcast RID transmits all information in the clear as plaintext, so Types 1 and 2 static IDs enable trivial correlation of patterns of use, unacceptable in many applications (e.g. package delivery routes of competitors).

1.1. UAS RID Uses

An ID is not an end in itself; it exists to enable lookups and provision of services complementing mere identification.

Minimal specified information must be made available to the public. Access to other data, e.g. UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized per policy. [F3411-19] specifies only how to get the UAS ID to the observer; how the observer can perform

these lookups, and how the registries first can be populated with information, is unspecified.

Dynamic establishment of secure communications between the observer and the UAS pilot seems to have been contemplated by the FAA UAS ID and Tracking Aviation Rulemaking Committee (ARC) in their [Recommendations], but it is not addressed in any of the subsequent proposed regulations or technical specifications.

Using UAS RID to facilitate related services, such as Detect And Avoid (DAA) and other applications of Vehicle to Vehicle or Vehicle to Infrastructure (V2V, V2I, collectively V2X) communications, is an obvious application. This is explicitly contemplated in the FAA NPRM, but has been omitted from [F3411-19]. DAA has been explicitly declared out of scope in ASTM working group discussions, based on a distinction between RID as a security standard vs DAA as a safety application.

1.2. UAS RID Design Considerations

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by observers of already ubiquitous mobile devices (smartphones and tablets). UA onboard RID devices are severely constrained in Cost, Size, Weight and Power ($SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and observer receive RID capabilities.

To accommodate the most severely constrained cases, all these conspire to motivate system design decisions, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges. Heavyweight security protocols are infeasible, yet trustworthiness of UAS RID information is essential. Under [F3411-19], even the most basic datum, the UAS ID string (typically number) itself can be merely an unsubstantiated claim.

1.3. DRIP Goals

DRIP will enable leveraging existing Internet resources (standard protocols, services, infrastructure and business models) to meet UAS RID and closely related needs. DRIP will specify how to apply IETF standards, complementing [F3411-19] and other external standards, to satisfy UAS RID requirements. DRIP will update existing and develop new protocol standards as needed to accomplish the foregoing.

This document will outline the UAS RID architecture into which DRIP must fit, and an architecture for DRIP itself. This includes presenting the gaps between the CAAs' Concepts of Operations and [F3411-19] as it relates to use of Internet technologies and UA direct RF communications. Issues include, but are not limited to:

* Trustworthy Remote ID and trust in RID messages

* Privacy in RID messages (PII protection)

* UA -> Ground communications including Broadcast RID

* Broadcast RID 'harvesting' and secure forwarding into the UTM

* Secure UAS -> Net-RID SP communications

2. Terms and Definitions

2.1. Requirements Terminology

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Additional Definitions

Most terminology needed in the DRIP context is introduced in the paired Requirements document (currently draft-card-drip-reqs).

CS-RID
: Crowd Sourced Remote Identification. An optional DRIP WG service

that gateways Broadcast RID to Network RID, and supports verification of RID position/velocity claims with independent measurements (e.g. by multilateration), via a SDSP.

HI
: Host Identity. The public key portion of an asymmetric key pair from HIP. In this document it is assumed that the HI is based on an EdDSA25519 key pair. This is supported by new crypto defined in [I-D.moskowitz-hip-new-crypto].

HIP
: Host Identity Protocol. The origin of HI, HIT, and HHIT, required for DRIP. Optional full use of HIP enables additional DRIP functionality.

HHIT
: Hierarchical Host Identity Tag. A HIT with extra information not found in a standard HIT. Defined in [I-D.moskowitz-hip-hierarchical-hit].

HIT
: Host Identity Tag. A 128 bit handle on the HI. Defined in HIPv2 [RFC7401].

3. Entities and their Interfaces

Any DRIP WG solutions for UAS RID must fit into the UTM (or U-space) system. This implies interaction with entities including UA, GCS, USS, Net-RID SP, Net-RID DP, Observers, Operators, Pilots In Command, Remote Pilots, possibly SDSP, etc. The only additional entities introduced in this document are registries, required but not specified by the regulations and [RFC7401], and optionally CS-RID

SDSP and Finder nodes. The DRIP WG may yet introduce other entities if/as needed.

UAS registries hold both public and private UAS information. The public information is primarily pointers to the repositories of, and keys for looking up, the private information. Given these different uses, and to improve scalability, security and simplicity of administration, the public and private information can be stored in different registries, indeed different types of registry.

3.1. Private Information Registry

3.1.1. Background

The private information required for UAS RID is similar to that required for Internet domain name registration. Thus a DRIP RID solution can leverage existing Internet resources: registration protocols, infrastructure and business models, by fitting into an ID structure compatible with DNS names. This implies some sort of hierarchy, for scalability, and management of this hierarchy. It is expected that the private registry function will be provided by the same organizations that run USS, and likely integrated with USS.

3.1.2. Proposed Approach

A DRIP UAS ID MUST be amenable to handling as an Internet domain name (at an arbitrary level in the hierarchy), MUST be registered in at least a pseudo-domain (e.g. .ip6 for reverse lookup), and MAY be registered as a sub-domain (for forward lookup).

A DRIP private information registry MUST support essential Internet domain name registry operations (e.g. add, delete, update, query) using interoperable open standard protocols. It SHOULD support the Extensible Provisioning Protocol (EPP) and the Registry Data Access Protocol (RDAP) with access controls. It MAY use XACML to specify those access controls. It MUST be listed in a DNS: that DNS MAY be private; but absent any compelling reasons for use of private DNS, SHOULD be the definitive public Internet DNS hierarchy. The DRIP private information registry in which a given UAS is registered MUST

be locatable, starting from the UAS ID, using the methods specified

in [RFC7484].

3.2. Public Information Registry

3.2.1. Background

The public information required to be made available by UAS RID is transmitted as clear plaintext to local observers in Broadcast RID and is served to a client by a Net-RID DP in Network RID. Therefore, while IETF can offer e.g. [RFC6280] as one way to implement Network RID, the only public information required to support essential DRIP functions for UAS RID is that required to look up Internet domain hosts, services, etc.

3.2.2. Proposed Approach

A DRIP public information registry MUST be a standard DNS server, in the definitive public Internet DNS hierarchy. It MUST support NS, MX, SRV, TXT, AAAA, PTR, CNAME and HIP RR types.

3.3. CS-RID concept

ASTM anticipated that regulators would require both Broadcast RID and Network RID for large UAS, but allow RID requirements for small UAS to be satisfied with the operator's choice of either Broadcast RID or Network RID. The EASA initially specified Broadcast RID for UAS of essentially all UAS and is now considering Network RID also. The FAA NPRM requires both for Standard RID and specifies Broadcast RID only for Limited RID. One obvious opportunity is to enhance the architecture with gateways from Broadcast RID to Network RID. This provides the best of both and gives regulators and operators flexibility. Such gateways could be pre-positioned (e.g. around airports and other sensitive areas) and/or crowdsourced (as nothing more than a smartphone with a suitable app is needed). Gateways can also perform multilateration to provide independent measurements of UA position, which is otherwise entirely operator self-reported in UAS RID and UTM. CS-RID would be an option, beyond baseline DRIP functionality; if implemented, it adds 2 more entity types.

3.3.1. Proposed optional CS-RID SDSP

A CS-RID SDSP MUST appear (i.e. present the same interface) to a Net-RID SP as a Net-RID DP. A CS-RID SDSP MUST appear to a Net-RID DP as a Net-RID SP. A CS-RID SDSP MUST NOT present a standard GCS-facing interface as if it were a Net-RID SP. A CS-RID SDSP MUST NOT present a standard client-facing interface as if it were a Net-RID DP. A CS-RID SDSP MUST present a TBD interface to a CS-RID Finder; this

interface SHOULD be based upon but readily distinguishable from that between a GCS and a Net-RID SP.

3.3.2. Proposed optional CS-RID Finder

A CS-RID Finder MUST present a TBD interface to a CS-RID SDSP; this interface SHOULD be based upon but readily distinguishable from that between a GCS and a Net-RID SP. A CS-RID Finder must implement, integrate, or accept outputs from, a Broadcast RID receiver. A CS-RID Finder MUST NOT interface directly with a GCS, Net-RID SP, Net-RID DP or Network RID client.

4. Identifiers

4.1. Background

A DRIP UA ID needs to be "Trustworthy". This means that within the framework of the RID messages, an observer can establish that the RID used does uniquely belong to the UA. That the only way for any other UA to assert this RID would be to steal something from within the UA. The RID is self-generated by the UAS (either UA or GCS) and registered with the USS.

Within the limitations of Broadcast RID, this is extremely challenging as:

* An RID can at most be 20 characters

* The ASTM Basic RID message (the message containing the RID) is 25 characters; only 3 characters are currently unused

* The ASTM Authentication message, with some changes from [F3411-19] can carry 224 bytes of payload.

Standard approaches like X.509 and PKI will not fit these constraints, even using the new EdDSA algorithm. An example of a technology that will fit within these limitations is an enhancement on the Host Identity Tag (HIT) HIPv2 [RFC7401] as defined in HHIT [I-D.moskowitz-hip-hierarchical-hit].

By using the EdDSA HHIT suite, self-assertions of the RID can be done in as little as 84 bytes. Third-party assertions can be done in 200 bytes. An observer would need Internet access to validate a self-assertion claim. A third-party assertion can be validated via a small credential cache in a disconnected environment. This third-party assertion is possible when the third-party also uses HHITs for

its identity and the UA has the public key for that HHIT.

4.2. Proposed Approach

A DRIP UAS ID MUST be a HHIT. It SHOULD be self-generated by the UAS (either UA or GCS) and MUST be registered with the Private Information Registry identified in its hierarchy fields. Each UAS ID HHIT MUST NOT be used more than once, with one exception as follows.

Each UA MAY be assigned, by its manufacturer, a single HI and derived HHIT encoded as a hardware serial number per [CTA2063A]. Such a static HHIT SHOULD be used only to bind one-time use UAS IDs (other HHITs) to the unique UA. Depending upon implementation, this may leave a HI private key in the possession of the manufacturer (see Security Considerations).

Each UA equipped for Broadcast RID MUST be provisioned not only with its HHIT but also with the HI public key from which the HHIT was derived and the corresponding private key, to enable message signature. Each UAS equipped for Network RID MUST be provisioned likewise; the private key SHOULD reside only in the ultimate source of Network RID messages (i.e. on the UA itself if the GCS is merely relaying rather than sourcing Network RID messages). Each observer device MUST be provisioned with public keys of the UAS RID root registries and MAY be provisioned with public keys or certificates for subordinate registries.

Operators and Private Information Registries MUST possess and other UTM entities MAY possess UAS ID style HHITs. When present, such HHITs SHOULD be used with HIP to strongly mutually authenticate and optionally encrypt communications.

5. Proposed Transactions

Each Operator MUST generate a "HIo" and derived "HHITo", register them with a Private Information Registry along with whatever Operator data (inc. PII) is required by the cognizant CAA and the registry, and obtain a certificate "Cro" signed with "HIr(priv)" proving such registration.

To add an UA, an Operator MUST generate a "HIa" and derived "HHITa",

create a certificate "Coa" signed with "HIo(priv)" to associate the UA with its Operator, register them with a Private Information Registry along with whatever UAS data is required by the cognizant CAA and the registry, obtain a certificate "Croa" signed with "HIr(priv)" proving such registration, and obtain a certificate "Cra" signed with "HIr(priv)" proving UA registration in that specific registry while preserving Operator privacy. The operator then MUST provision the UA with "HIa", "HIa(priv)", "HHITa" and "Cra".

UA engaging in Broadcast RID MUST use "HIa(priv)" to sign Auth Messages and MUST periodically broadcast "Cra". UAS engaging in Network RID MUST use "HIa(priv)" to sign Auth Messages. Observers MUST use "HIa" from received "Cra" to verify received Broadcast RID Auth messages. Observers without Internet connectivity MAY use "Cra" to identify the trust class of the UAS based on known registry vetting. Observers with Internet connectivity MAY use "HHITa" to perform lookups in the Public Information Registry and MAY then query the Private Information Registry, which MUST enforce AAA policy on Operator PII and other sensitive information.

6. IANA Considerations

It is likely that an IPv6 prefix will be needed for the HHIT (or other identifier) space: this should be coordinated with ICAO; this will be specified in other drafts.

7. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. A manufacturer that embeds a private key in an UA may have retained a copy. A manufacturer whose UA are configured by a closed source application on the GCS which communicates over the Internet with the factory may be sending a copy of a UA or GCS self-generated key back to the factory. Compromise of a registry private key could do widespread harm. Key revocation procedures are as yet to be determined. These risks are in addition to those involving Operator key management practices.

8. Acknowledgments

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM and proposed IETF DRIP WG efforts. The work of ASTM F38.02 in balancing the interests of diverse stakeholders is essential to the necessary rapid and widespread deployment of UAS RID.

Appendix A was provided by Shuai Zhao of Tencent.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,

DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7484] Blanchet, M., "Finding the Authoritative Registration Data (RDAP) Service", RFC 7484, DOI 10.17487/RFC7484, March 2015, <https://www.rfc-editor.org/info/rfc7484>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[ATIS-I-0000074]
ATIS, "Report on UAS in 3GPP", <https://access.atis.org/apps/group_public/download.php/48760/ATIS-I-0000074.pdf>.

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", September 2019.

[Delegated]
European Union Aviation Safety Agency (EASA), "EU Commission Delegated Regulation 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country

operators of unmanned aircraft systems", March 2019.

[F3411-19] ASTM, "Standard Specification for Remote ID and Tracking", December 2019.

[I-D.moskowitz-hip-hierarchical-hit]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-04, 3 March 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-04>.

[I-D.moskowitz-hip-new-crypto]
Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-04, 23 January 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-new-crypto-04>.

[Implementing]
European Union Aviation Safety Agency (EASA), "EU Commission Implementing Regulation 2019/947 of 24 May 2019

on the rules and procedures for the operation of unmanned aircraft", May 2019.

[LANNC] United States Federal Aviation Administration (FAA), "Low Altitude Authorization and Notification Capability", <https://www.faa.gov/uas/programs_partnerships/data_exchange/>.

[NPRM] United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019.

[Recommendations]
FAA UAS Identification and Tracking Aviation Rulemaking Committee, "UAS ID and Tracking ARC Recommendations Final Report", September 2017.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally

Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, DOI 10.17487/RFC6280, July 2011, <https://www.rfc-editor.org/info/rfc6280>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[TS-22.825] 3GPP, "UAS RID requirement study", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3527>.

[TS-36.777] 3GPP, "UAV service in the LTE network", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3231>.

[U-Space] European Organization for the Safety of Air Navigation (EUROCONTROL), "U-space Concept of Operations", October 2019, <https://www.sesarju.eu/sites/default/files/documents/u-space/CORUS%20ConOps%20vol2.pdf>.

Appendix A. Overview of Unmanned Aircraft Systems (UAS) Traffic Management (UTM)

A.1. Operation Concept

The National Aeronautics and Space Administration (NASA) and FAAs' effort of integrating UAS's operation into the national airspace system (NAS) leads to the development of the concept of UTM and the ecosystem around it. The UTM concept was initially presented in 2013. The eventual development and implementation are conducted by the UTM research transition team (RTT) which is the joint workforce

by FAA and NASA. World efforts took place afterward. The Single European Sky ATM Research (SESAR) started the CORUS project to research its UTM counterpart concept, namely [U-Space]. This effort is led by the European Organization for the Safety of Air Navigation (Eurocontrol).

Both NASA and SESAR have published the UTM concept of operations to guide the development of their future air traffic management (ATM) system and make sure safe and efficient integrations of manned and unmanned aircraft into the national airspace.

The UTM composes of UAS operation infrastructure, procedures and local regulation compliance policies to guarantee UAS's safe integration and operation. The main functionality of a UTM includes but not limited to provides means of communication between UAS operators and service providers and a platform to facilitate communication among UAS service providers.

A.2. UAS service supplier (USS)

A USS plays an important role to fulfill the key performance indicators (KPIs) that a UTM has to offer. Such Entity acts as a proxy between UAS operators and UTM service providers. It provides services like real-time UAS traffic monitor and planning, aeronautical data archiving, airspace and violation control, interacting with other third-party control entities, etc. A USS can coexist with other USS(s) to build a large service coverage map which can load-balance, relay and share UAS traffic information.

The FAA works with UAS industry shareholders and promotes the Low Altitude Authorization and Notification Capability [LANNC] program which is the first implementation to realize UTM's functionality. The LAANC program can automate the UAS's fly plan application and approval process for airspace authorization in real-time by checking against multiple aeronautical databases such as airspace classification and fly rules associated with it, FAA UAS facility

map, special use airspace, Notice to airman (NOTAM) and Temporary flight rule (TFR).

A.3. UTM Use cases for UAS operation

This section illustrates a couple of use case scenarios where UAS's participation in UTM has significant safety improvement.

1. For a UAS participating in UTM and takeoff or land in a controlled airspace (ex. Class Bravo, Charlie, Delta and Echo in United Stated), the USS where UAS is currently communicating with is responsible for UAS's registration, authenticating the UAS's fly plan by checking against designated UAS fly map database, obtaining the air traffic control (ATC) authorization and monitor the UAS fly path in order to maintain safe boundary and follow the pre-authorized route.

2. For a UAS participating in UTM and take off or land in an uncontrolled airspace (ex. Class Golf in the United States), pre-fly authorization must be obtained from a USS when operating beyond-visual-of-sight (BVLOS) operation. The USS either accepts or rejects received intended fly plan from the UAS. Accepted UAS operation may share its current fly data such as GPS position and altitude to USS. The USS may keep the UAS flight status near real-time and may keep it as a record for overall airspace air traffic monitor.

A.4. Overview UAS Remote ID (RID) and RID Standardization

A RID is an application enabler for a UAS to be identified by a UTM/USS or third parties entities such as law enforcement. Many safety and other considerations dictate that UAS be remotely identifiable. CAAs worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The FAA has published a Notice of Proposed Rule Making [NPRM]. CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

3GPP provides UA service in the LTE network since release 15 in published technical specification [TS-36.777]. Start from its release 16, it completed the UAS RID requirement study in [TS-22.825] and proposed use cases in the mobile network and the services that can be offered based on RID and ongoing release 17 specification works on enhanced UAS service requirement and provides the protocol and application architecture support which is applicable for both 4G and 5G network. ATIS's recent report [ATIS-I-0000074] proposes architecture approaches for the 3GPP network to support UAS and one

of which is put RID in higher 3GPP protocol stack such as using ASTM remote ID [F3411-19].

Authors' Addresses

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com

Shuai Zhao
Tencent
CA
United States of America

Email: shuaiizhao@tencent.com