Internet Engineering Task Force (IETF)
Request for Comments: 9434
Category: Informational
ISSN: 2070-1721

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao, Ed.
Intel
A. Gurtov
Linkping University

July 2023

Drone Remote Identification Protocol (DRIP) Architecture

Abstract

This document describes an architecture for protocols and services to support Unmanned Aircraft System Remote Identification and tracking (UAS RID), plus UAS-RID-related communications. This architecture adheres to the requirements listed in the Drone Remote Identification Protocol (DRIP) Requirements document (RFC 9153).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9434.

Table of Contents

1. Introduction

This document describes an architecture for protocols and services to support Unmanned Aircraft System Remote Identification and tracking (UAS RID), plus UAS-RID-related communications. The architecture takes into account both current (including proposed) regulations and non-IETF technical standards.

The architecture adheres to the requirements listed in the DRIP Requirements document [RFC9153] and illustrates how all of them can be met, except for GEN-7 QoS, which is left for future work. The requirements document provides an extended introduction to the problem space and use cases. Further, this architecture document frames the DRIP Entity Tag (DET) [RFC9374] within the architecture.

1.1. Overview of UAS RID and Its Standardization

UAS RID is an application that enables UAS to be identified by UAS Traffic Management (UTM), UAS Service Suppliers (USS) (Appendix A), and third-party entities, such as law enforcement. Many considerations (e.g., safety and security) dictate that UAS be remotely identifiable.

Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. CAAs currently promulgate performance-based regulations that do not

specify techniques but rather cite industry consensus technical standards as acceptable means of compliance.

USA Federal Aviation Administration (FAA)
: The FAA published a Notice of Proposed Rule Making [NPRM] in 2019 and thereafter published a "Final Rule" in 2021 [FAA_RID], imposing requirements on UAS manufacturers and operators, both commercial and recreational. The rule states that Automatic Dependent Surveillance Broadcast (ADS-B) Out and transponders cannot be used to satisfy the UAS RID requirements on UAS to which the rule applies (see Appendix B).

European Union Aviation Safety Agency (EASA)
: In pursuit of the "U-space" concept of a single European airspace safely shared by manned and unmanned aircraft, the EASA published a [Delegated] regulation in 2019, imposing requirements on UAS manufacturers and third-country operators, including but not limited to UAS RID requirements. The same year, the EASA also published a regulation [Implementing], laying down detailed rules and procedures for UAS operations and operating personnel, which then was updated in 2021 [Implementing_update]. A Notice of Proposed Amendment [NPA] was published in 2021 to provide more information about the development of acceptable means of compliance and guidance material to support U-space regulations.

American Society for Testing and Materials (ASTM)
: ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041 developed an ASTM standard [F3411-22a], titled "Standard Specification for Remote ID and Tracking".

  ASTM defines one set of UAS RID information and two means, Media Access Control (MAC) layer broadcast and IP layer network, of communicating it. If a UAS uses both communication methods, the same information must be provided via both means. [F3411-22a] is the technical standard basis of the Means Of Compliance (MOC) specified in [F3586-22]. The FAA has accepted [F3586-22] as a MOC to the FAA’s UAS RID Final Rule [FAA_RID], with some caveats, as per [MOC-NOA]. Other CAAs are expected to accept the same or other MOCs likewise based on [F3411-22a].

3rd Generation Partnership Project (3GPP)
: With Release 16, the 3GPP completed the UAS RID requirement study [TR-22.825] and proposed a set of use cases in the mobile network and services that can be offered based on UAS RID. The Release 17 study [TR-23.755] and specification [TS-23.255] focus on enhanced UAS service requirements and provide the protocol and application architecture support that will be applicable for both 4G and 5G networks. The study of Further Architecture Enhancement for Uncrewed Aerial Vehicles (UAV) and Urban Air Mobility (UAM) in Release 18 [FS_AEUA] further enhances the communication mechanism between UAS and USS/UTM. The DET in Section 3 may be used as the 3GPP CAA-level UAS ID for RID purposes.

1.2. Overview of Types of UAS Remote ID

This specification introduces two types of UAS Remote IDs as defined in ASTM [F3411-22a].

1.2.1. Broadcast RID

[F3411-22a] defines a set of UAS RID messages for direct, one-way broadcast transmissions from the Unmanned Aircraft (UA) over Bluetooth or Wi-Fi. These are currently defined as MAC layer messages. Internet (or other Wide Area Network) connectivity is only needed for UAS registry information lookup by Observers using the

directly received UAS ID. Broadcast RID should be functionally usable in situations with no Internet connectivity.

The minimum Broadcast RID data flow is illustrated in Figure 1.

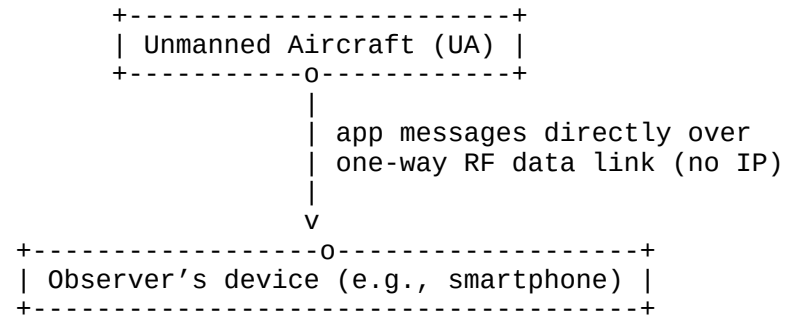


Figure 1: Minimum Broadcast RID Data Flow

Broadcast RID provides information only about UA within direct Radio Frequency (RF) Line Of Sight (LOS), typically similar to Visual LOS (VLOS), with a range up to approximately 1 km. This information may be 'harvested' from received broadcasts and made available via the Internet, enabling surveillance of areas too large for local direct visual observation or direct RF link-based identification (see Section 6).

1.2.2. Network RID

[F3411-22a], using the same data dictionary that is the basis of Broadcast RID messages, defines a Network Remote Identification (Net-RID) data flow as follows.

* The information to be reported via UAS RID is generated by the UAS. Typically, some of this data is generated by the UA and some by the Ground Control Station (GCS), e.g., their respective locations derived from the Global Navigation Satellite System (GNSS).

* The information is sent by the UAS (UA or GCS) via unspecified means to the cognizant Network Remote Identification Service Provider (Net-RID SP), typically the USS under which the UAS is operating if it is participating in UTM.

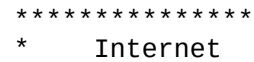
* The Net-RID SP publishes, via the Discovery and Synchronization Service (DSS) over the Internet, that it has operations in various 4-D airspace volumes (Section 2.2 of [RFC9153]), describing the volumes but not the operations.

* An Observer's device, which is expected but not specified to be based on the Web, queries a Network Remote Identification Display Provider (Net-RID DP), typically also a USS, about any operations in a specific 4-D airspace volume.

* Using fully specified Web-based methods over the Internet, the Net-RID DP queries all Net-RID SPs that have operations in volumes intersecting that of the Observer's query for details on all such operations.

* The Net-RID DP aggregates information received from all such Net-RID SPs and responds to the Observer's query.

The minimum Net-RID data flow is illustrated in Figure 2:



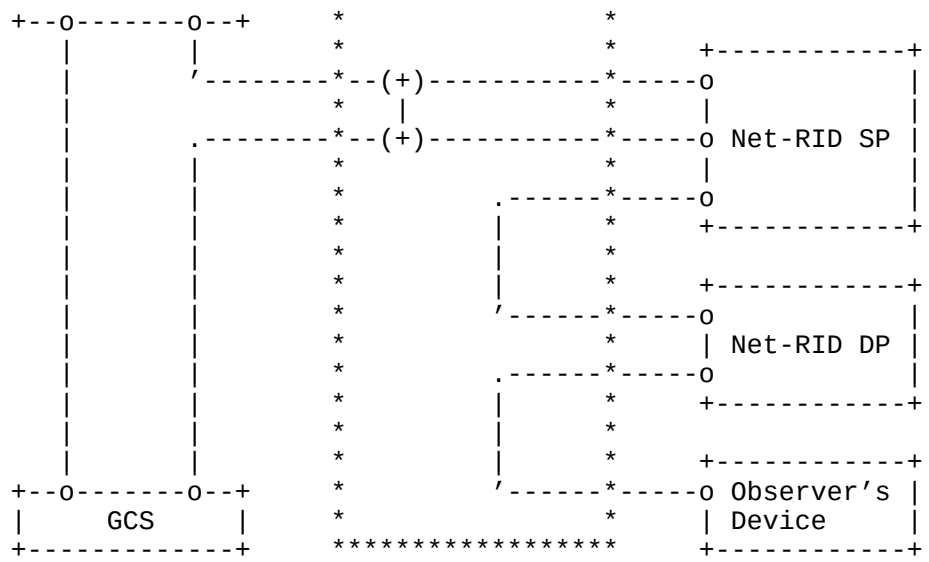


Figure 2: Minimum Net-RID Data Flow

Command and Control (C2) must flow from the GCS to the UA via some path. Currently (in the year 2023), this is typically a direct RF link; however, with increasing Beyond Visual Line Of Sight (BVLOS) operations, it is expected to often be a wireless link at either end with the Internet between.

Telemetry (at least the UA's position and heading) flows from the UA to the GCS via some path, typically the reverse of the C2 path. Thus, UAS RID information pertaining to both the GCS and the UA can be sent by whichever has Internet connectivity to the Net-RID SP, typically the USS managing the UAS operation.

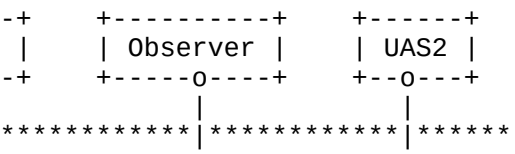
The Net-RID SP forwards UAS RID information via the Internet to subscribed Net-RID DPs, typically the USS. Subscribed Net-RID DPs then forward RID information via the Internet to subscribed Observer devices. Regulations require and [F3411-22a] describes UAS RID data elements that must be transported end to end from the UAS to the subscribed Observer devices.

[F3411-22a] prescribes the protocols between the Net-RID SP, Net-RID DP, and DSS. It also prescribes data elements (in JSON) between the Observer and the Net-RID DP. DRIP could address standardization of secure protocols between the UA and the GCS (over direct wireless and Internet connection), between the UAS and the Net-RID SP, and/or between the Net-RID DP and Observer devices.

Neither link-layer protocols nor the use of links (e.g., the link often existing between the GCS and the UA) for any purpose other than carriage of UAS RID information are in the scope of Network RID [F3411-22a].

1.3. Overview of USS Interoperability

With Net-RID, there is direct communication between each UAS and its USS. Multiple USS exchange information with the assistance of a DSS so all USS collectively have knowledge about all activities in a 4-D airspace. The interactions among an Observer, multiple UAS, and their USS are shown in Figure 3.



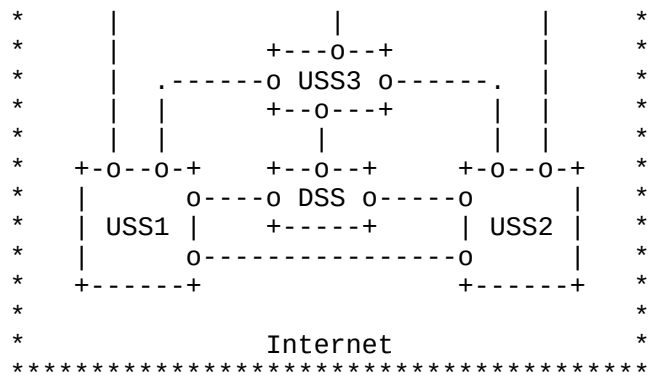
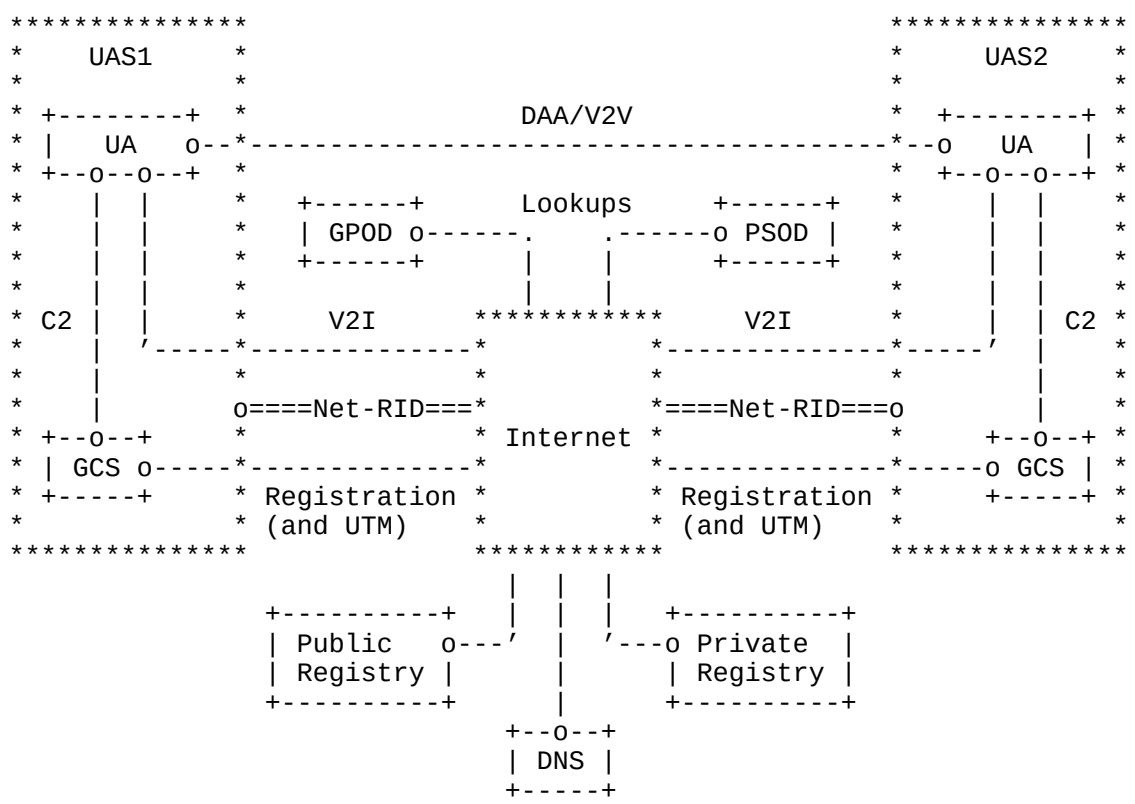


Figure 3: Interactions Between Observers, UAS, and USS

1.4. Overview of DRIP Architecture

Figure 4 illustrates a global UAS RID usage scenario. Broadcast RID links are not shown, as they reach from any UA to any listening receiver in range and thus would obscure the intent of the figure. Figure 4 shows, as context, some entities and interfaces beyond the scope of DRIP (as currently (2023) chartered). Multiple UAS are shown, each with its own UA controlled by its own GCS, potentially using the same or different USS, with the UA potentially communicating directly with each other (V2V), especially for low-latency, safety-related purposes (DAA).



DAA: Detect And Avoid
GPOD: General Public Observer Device
PSOD: Public Safety Observer Device
V2I: Vehicle-to-Infrastructure
V2V: Vehicle-to-Vehicle

Figure 4: Global UAS RID Usage Scenario

| Informative note: See [RFC9153] for detailed definitions.

DRIP is meant to leverage existing Internet resources (standard protocols, services, infrastructures, and business models) to meet UAS RID and closely related needs. DRIP will specify how to apply IETF standards, complementing [F3411-22a] and other external standards, to satisfy UAS RID requirements.

This document outlines the DRIP architecture in the context of the UAS RID architecture. This includes closing the gaps between the CAAs' concepts of operations and [F3411-22a] as it relates to the use of Internet technologies and UA-direct RF communications. Issues include, but are not limited to:

* the design of trustworthy remote identifiers required by GEN-1 (Section 3), especially but not exclusively for use as single-use session IDs,

* mechanisms to leverage the Domain Name System (DNS) [RFC1034] for registering and publishing public and private information (see Sections 4.1 and 4.2), as required by REG-1 and REG-2,

* specific authentication methods and message payload formats to enable verification that Broadcast RID messages were sent by the claimed sender (Section 5) and that the sender is in the claimed DRIP Identity Management Entity (DIME) (see Sections 4 and 5), as required by GEN-2,

* harvesting Broadcast RID messages for UTM inclusion, with the optional DRIP extension of Crowdsourced Remote ID (CS-RID) (Section 6), using the DRIP support for gateways required by GEN-5 [RFC9153],

* methods for instantly establishing secure communications between an Observer and the pilot of an observed UAS (Section 7), using the DRIP support for dynamic contact required by GEN-4 [RFC9153], and

* privacy in UAS RID messages (personal data protection) (Section 10).

This document should serve as a main point of entry into the set of IETF documents addressing the basic DRIP requirements.

2. Terms and Definitions

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.

To encourage comprehension necessary for adoption of DRIP by the intended user community, the UAS community's norms are respected herein.

This document uses terms defined in [RFC9153].

Some of the acronyms have plural forms that remain the same as their singular forms, e.g., "UAS" can expand to "Unmanned Aircraft System" (singular) or "Unmanned Aircraft Systems" (plural), as appropriate for the context. This usage is consistent with Section 2.2 of [RFC9153].

2.1. Additional Abbreviations

DET: DRIP Entity Tag

EdDSA: Edwards-curve Digital Signature Algorithm

HHIT: Hierarchical HIT

HI: Host Identity

HIP: Host Identity Protocol

HIT: Host Identity Tag

2.2. Additional Definitions

This section introduces the terms "Claim", "Evidence", "Endorsement", and "Certificate", as used in DRIP. A DRIP certificate has a different context compared with security certificates and Public Key Infrastructure used in X.509.

Claim:
A claim shares the same definition as a claim in Remote ATtestation procedureS (RATS) [RFC9334]; it is a piece of asserted information, sometimes in the form of a name/value pair. It could also been seen as a predicate (e.g., "X is Y", "X has property Y", and most importantly "X owns Y" or "X is owned by Y").

Evidence:
Evidence in DRIP borrows the same definition as in RATS [RFC9334], that is, a set of claims.

Endorsement:
An Endorsement is inspired from RATS [RFC9334]; it is a secure (i.e., signed) statement vouching the integrity and veracity of evidence.

Certificate:
A certificate in DRIP is an endorsement, strictly over identity information, signed by a third party. This third party should be one with no stake in the endorsement over which it is signing.

DRIP Identity Management Entity (DIME):
A DIME is an entity that performs functions similar to a domain registrar/registry. A DIME vets Claims and/or Evidence from a registrant and delivers back Endorsements and/or Certificates in response. It is a high-level entity in the DRIP registration/provisioning process that can hold the role of HHIT Domain Authority (HDA), Registered Assigning Authority (RAA), or root of trust (typically the HHIT prefix owner or DNS apex owner) for DETs.

3. HHIT as the DRIP Entity Identifier

This section describes the DRIP architectural approach to meeting the basic requirements of a DRIP entity identifier within the external technical standard ASTM [F3411-22a] and regulatory constraints. It justifies and explains the use of Hierarchical Host Identity Tags (HHITs) [RFC9374] as self-asserting IPv6 addresses suitable as a UAS ID type and, more generally, as trustworthy multipurpose remote identifiers.

Self-asserting in this usage means that, given the Host Identity (HI), the HHIT Overlay Routable Cryptographic Hash IDentifier (ORCHID) construction (see Section 3.5 of [RFC9374]), and a signature of the DIME on the HHIT and HI, the HHIT can be verified by the receiver as a trusted UAS ID. The explicit registration hierarchy within the HHIT provides registration discovery (managed by a DIME) to either yield the HI for third-party (seeking UAS ID endorsement) validation or prove that the HHIT and HI have been registered

uniquely.

3.1. UAS Remote Identifiers Problem Space

A DRIP entity identifier needs to be "Trustworthy" (see DRIP requirements GEN-1, ID-4, and ID-5 in [RFC9153]). This means that given a sufficient collection of UAS RID messages, an Observer can establish that the identifier claimed therein uniquely belongs to the claimant. To satisfy DRIP requirements and maintain important security properties, the DRIP identifier should be self-generated by the entity it names (e.g., a UAS) and registered (e.g., with a USS; see DRIP requirements GEN-3 and ID-2).

However, Broadcast RID, especially its support for Bluetooth 4, imposes severe constraints. A previous revision of the ASTM UAS RID, [F3411-19], allowed a UAS ID of types (1, 2, and 3), each of 20 bytes. [F3411-22a] adds type 4, Specific Session ID, for other Standards Development Organizations (SDOs) to extend ASTM UAS RID. Type 4 uses one byte to index the Specific Session ID subtype, leaving 19 bytes (see ID-1 of DRIP Requirements [RFC9153]). As described in Section 3 of [RFC9153], ASTM has allocated Specific Session ID subtype 1 to IETF DRIP.

The maximum ASTM UAS RID Authentication Message payload is 201 bytes each for Authentication Types 1, 2, 3, and 4. [F3411-22a] adds Authentication Type 5 for other SDOs (including the IETF) to extend ASTM UAS RID with Specific Authentication Methods (SAMs). With Type 5, one of the 201 bytes is consumed to index the SAM Type, leaving only 200 bytes for DRIP authentication payloads, including one or more DRIP entity identifiers and associated authentication data.

3.2. HHIT as a Cryptographic Identifier

The only (known to the authors at the time of writing) existing types of IP-address-compatible identifiers cryptographically derived from the public keys of the identified entities are Cryptographically Generated Addresses (CGAs) [RFC3972] and Host Identity Tags (HITs) [RFC7401]. CGAs and HITs lack registration/retrieval capability. To provide this, each HHIT embeds plaintext information designating the hierarchy within which it is registered, a cryptographic hash of that information concatenated with the entity’s public key, etc. Although hash collisions may occur, the DIME can detect them and reject registration requests rather than issue credentials, e.g., by enforcing a First Come First Served policy [RFC8126]. Preimage hash attacks are also mitigated through this registration process, locking the HHIT to a specific HI.

3.3. HHIT as a Trustworthy DRIP Entity Identifier

A Remote UAS ID that can be trustworthy for use in Broadcast RID can be built from an asymmetric key pair. In this method, the UAS ID is cryptographically derived directly from the public key. The proof of UAS ID ownership (verifiable endorsement versus mere claim) is guaranteed by signing this cryptographic UAS ID with the associated private key. The association between the UAS ID and the private key is ensured by cryptographically binding the public key with the UAS ID; more specifically, the UAS ID results from the hash of the public key. The public key is designated as the HI, while the UAS ID is designated as the HIT.

By construction, the HIT is statistically unique through the mandatory use of cryptographic hash functions with second-preimage resistance. The cryptographically bound addition of the hierarchy and a HHIT registration process provide complete, global HHIT uniqueness. This registration forces the attacker to generate the same public key rather than a public key that generates the same

HHIT. This is in contrast to general IDs (e.g., a Universally Unique Identifier (UUID) or device serial number) as the subject in an X.509 certificate.

A 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.

A UAS equipped for DRIP-enhanced Network RID MUST be provisioned likewise; the private key resides only in the ultimate source of Network RID messages. If the GCS is the source of the Network RID messages, the GCS MUST hold the private key. If the UA is the source of the Network RID messages and they are being relayed by the GCS, the UA MUST hold the private key, just as a UA that directly connects to the network rather than through its GCS.

Each Observer device functioning with Internet connectivity MAY be provisioned either with public keys of the DRIP identifier root registries or certificates for subordinate registries; each Observer device that needs to operate without Internet connectivity at any time MUST be so provisioned.

HHITs can also be used throughout the USS/UTM system. Operators and Private Information Registries, as well as other UTM entities, can use HHITs for their IDs. Such HHITs can facilitate DRIP security functions, such as those used with HIP, to strongly mutually authenticate and encrypt communications.

A self-endorsement of a HHIT used as a UAS ID can be done in as little as 88 bytes when Ed25519 [RFC8032] is used by only including the 16-byte HHIT, two 4-byte timestamps, and the 64-byte Ed25519 signature.

Ed25519 [RFC8032] is used as the HHIT mandatory-to-implement signing algorithm, as GEN-1 and ID-5 [RFC9153] can best be met by restricting the HI to 32 bytes. A larger public key would rule out the offline endorsement feature that fits within the 200-byte Authentication Message maximum length. Other algorithms that meet this 32-byte constraint can be added as deemed needed.

A DRIP identifier can be assigned to a UAS as a static HHIT by its manufacturer, such as a single HI and derived HHIT encoded as a hardware serial number, per [CTA2063A]. Such a static HHIT SHOULD only be used to bind one-time-use DRIP identifiers to the unique UA. Depending upon implementation, this may leave a HI private key in the possession of the manufacturer (see also Section 9).

In general, Internet access may be needed to validate Endorsements or Certificates. This may be obviated in the most common cases (e.g., endorsement of the UAS ID), even in disconnected environments, by prepopulating small caches on Observer devices with DIME public keys and a chain of Endorsements or Certificates (tracing a path through the DIME tree). This is assuming all parties on the trust path also use HHITs for their identities.

3.4. HHIT for DRIP Identifier Registration and Lookup

UAS RID needs a deterministic lookup mechanism that rapidly provides actionable information about the identified UA. Given the size constraints imposed by the Bluetooth 4 broadcast media, the UAS ID itself needs to be a non-spoofable inquiry input into the lookup.

A DRIP registration process based on the explicit hierarchy within a HHIT provides manageable uniqueness of the HI for the HHIT. The hierarchy is defined in [RFC9374] and consists of 2 levels: an RAA and then an HDA. The registration within this hierarchy is the

defense against a cryptographic hash second-preimage attack on the HHIT (e.g., multiple HIs yielding the same HHIT; see Requirement ID-3 in [RFC9153]). The First Come First Served registration policy is adequate.

A lookup of the HHIT into the DIME provides the registered HI for HHIT proof of ownership and deterministic access to any other needed actionable information based on inquiry access authority (more details in Section 4.2).

4. DRIP Identifier Registration and Registries

DRIP registries hold both public and private UAS information (see PRIV-1 in [RFC9153]) resulting from the DRIP identifier registration process. Given these different uses, and to improve scalability, security, and simplicity of administration, the public and private information can be stored in different registries. This section introduces the public and private information registries for DRIP identifiers. In this section, for ease of comprehension, the registry functions are described (using familiar terminology) without detailing their assignment to specific implementing entities (or using unfamiliar jargon). Elsewhere in this document, and in forthcoming documents detailing the DRIP registration processes and entities, the more specific term "DRIP Identity Management Entity" (DIME) will be used. This DRIP identifier registration process satisfies the following DRIP requirements defined in [RFC9153]: GEN-3, GEN-4, ID-2, ID-4, ID-6, PRIV-3, PRIV-4, REG-1, REG-2, REG-3, and REG-4.

4.1. Public Information Registry

4.1.1. Background

The public information registry provides trustable information, such as endorsements of UAS RID ownership and registration with the HDA. Optionally, pointers to the registries for the HDA and RAA implicit in the UAS RID can be included (e.g., for HDA and RAA HHIT|HI used in endorsement signing operations). This public information will be principally used by Observers of Broadcast RID messages. Data on UAS that only use Network RID is available via an Observer’s Net-RID DP that would directly provide all public registry information. The Net-RID DP is the only source of information for a query on an airspace volume.

> | Note: In the above paragraph, | signifies concatenation of
> | information, e.g., X | Y is the concatenation of X and Y.

4.1.2. Public DRIP Identifier Registry

A DRIP identifier MUST be registered as an Internet domain name (at an arbitrary level in the hierarchy, e.g., in .ip6.arpa). Thus, the DNS can provide all the needed public DRIP information. A standardized HHIT Fully Qualified Domain Name (FQDN) can deliver the HI via a HIP Resource Record (RR) [RFC8005] and other public information (e.g., RAA and HDA PTRs and HIP Rendezvous Servers (RVSs) [RFC8004]). These public information registries can use DNSSEC to deliver public information that is not inherently trustable (e.g., everything other than endorsements).

This DNS entry for the HHIT can also provide a revocation service. For example, instead of returning the HI RR, it may return some record showing that the HI (and thus HHIT) has been revoked.

4.2. Private Information Registry

4.2.1. Background

The private information required for DRIP identifiers is similar to that required for Internet domain name registration. A DRIP identifier solution can leverage existing Internet resources, i.e., registration protocols, infrastructure, and business models, by fitting into a UAS ID structure compatible with DNS names. The HHIT hierarchy can provide the needed scalability and management structure. It is expected that the private information registry function will be provided by the same organizations that run a USS and likely integrated with a USS. The lookup function may be implemented by the Net-RID DPs.

4.2.2. Information Elements

When a DET is used as a UA's Session ID, the corresponding manufacturer-assigned serial number MUST be stored in a private information registry that can be identified uniquely from the DET. When a DET is used as either a UA's Session ID or a UA's manufacturer-assigned serial number, and the operation is being flown under UTM, the corresponding UTM-system-assigned Operational Intent Identifier SHOULD be so stored. Other information MAY be stored as such, and often must, to satisfy CAA regulations or USS operator policies.

4.2.3. Private DRIP Identifier Registry Methods

A DRIP private information registry supports essential registry operations (e.g., add, delete, update, and query) using interoperable open standard protocols. It can accomplish this by leveraging aspects of the Extensible Provisioning Protocol (EPP) [RFC5730] and the Registry Data Access Protocol (RDAP) [RFC7480] [RFC9082] [RFC9083]. The DRIP private information registry in which a given UAS is registered needs to be findable, starting from the UAS ID, using the methods specified in [RFC9224].

4.2.4. Alternative Private DRIP Registry Methods

A DRIP private information registry might be an access-controlled DNS (e.g., via DNS over TLS). Additionally, WebFinger [RFC7033] can be supported. These alternative methods may be used by a Net-RID DP with specific customers.

5. DRIP Identifier Trust

While the DRIP entity identifier is self-asserting, it alone does not provide the trustworthiness (i.e., non-repudiation, protection vs. spoofing, message integrity protection, scalability, etc.) essential to UAS RID, as justified in [RFC9153]. For that, it MUST be registered (under DRIP registries) and actively used by the party (in most cases the UA). A sender's identity cannot be proved merely by its possessing of a DRIP Entity Tag (DET) and broadcasting it as a claim that it belongs to that sender. Sending data signed using that HI's private key proves little, as it is subject to trivial replay attacks using previously broadcast messages. Only sending the DET and a signature on novel (i.e., frequently changing and unpredictable) data that can be externally validated by the Observer (such as a signed Location/Vector message that matches actually seeing the UA at the location and time reported in the signed message) proves that the observed UA possesses the private key and thus the claimed UAS ID.

The severe constraints of Broadcast RID make it challenging to satisfy UAS RID requirements. From received Broadcast RID messages and information that can be looked up using the received UAS ID in online registries or local caches, it is possible to establish levels of trust in the asserted information and the operator.

A combination of different DRIP Authentication Messages enables an Observer, without Internet connection (offline) or with (online), to validate a UAS DRIP ID in real time. Some messages must contain the relevant registration of the UA's DRIP ID in the claimed DIME. Some messages must contain sender signatures over both static (e.g., registration) and dynamically changing (e.g., current UA location) data. Combining these two sets of information, an Observer can piece together a chain of trust, including real-time evidence to make a determination on the UA's claims.

This process (combining the DRIP entity identifier, registries, and authentication formats for Broadcast RID) can satisfy the following DRIP requirements defined in [RFC9153]: GEN-1, GEN-2, GEN-3, ID-2, ID-3, ID-4, and ID-5.

6. Harvesting Broadcast Remote ID Messages for UTM Inclusion

ASTM anticipated that regulators would require both Broadcast RID and Network RID for large UAS but allow UAS 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 essentially all UAS and is now also considering Network RID. The FAA UAS RID Final Rules [FAA_RID] permit only Broadcast RID for rule compliance but still encourage Network RID for complementary functionality, especially in support of UTM.

One 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. It offers advantages over either form of UAS RID alone, i.e., greater fidelity than Network RID reporting of [FAA_RID] planned area operations, together with surveillance of areas too large for local direct visual observation and direct Radio Frequency Line Of Sight (RF-LOS) link-based Broadcast RID (e.g., a city or a national forest).

These gateways could be pre-positioned (e.g., around airports, public gatherings, and other sensitive areas) and/or crowdsourced (as nothing more than a smartphone with a suitable app is needed). Crowdsourcing can be encouraged by quid pro quo, providing CS-RID Surveillance Supplemental Data Service Provider (SDSP) outputs only to CS-RID Finders. As Broadcast RID media have a limited range, messages claiming sender (typically UA) locations far from a physical layer receiver thereof ("Finder" below, typically Observer device) should arouse suspicion of possible intent to deceive; a fast and computationally inexpensive consistency check can be performed (by the Finder or the Surveillance SDSP) on application layer data present in the gateway (claimed UA location vs physical receiver location), and authorities can be alerted to failed checks. CS-RID SDSPs can use messages with precise date/time/position stamps from the gateways to multilaterate UA locations, independent of the locations claimed in the messages, which are entirely self-reported by the operator in UAS RID and UTM, and thus are subject not only to natural time lag and error but also operator misconfiguration or intentional deception.

Multilateration technologies use physical layer information, such as precise Time Of Arrival (TOA) of transmissions from mobile transmitters at receivers with a priori precisely known locations, to estimate the locations of the mobile transmitters.

Further, gateways with additional sensors (e.g., smartphones with cameras) can provide independent information on the UA type and size, confirming or refuting those claims made in the UAS RID messages.

Sections 6.1 and 6.2 define two additional entities that are required

to provide this Crowdsourced Remote ID (CS-RID).

This approach satisfies the following DRIP requirements defined in [RFC9153]: GEN-5, GEN-11, and REG-1. As Broadcast messages are inherently multicast, GEN-10 is met for local-link multicast to multiple Finders (this is how multilateration is possible).

6.1. The CS-RID Finder

A CS-RID Finder is the gateway for Broadcast Remote ID Messages into UTM. It performs this gateway function via a CS-RID SDSP. A CS-RID Finder could implement, integrate, or accept outputs from a Broadcast RID receiver. However, it should not depend upon a direct interface with a GCS, Net-RID SP, Net-RID DP, or Net-RID client. It would present a new interface to a CS-RID SDSP, similar to but readily distinguishable from that which a UAS (UA or GCS) presents to a Net-RID SP.

6.2. The CS-RID SDSP

A CS-RID SDSP aggregates and processes (e.g., estimates UA locations using multilateration when possible) information collected by CS-RID Finders. A CS-RID SDSP should present the same interface to a Net-RID SP as it does to a Net-RID DP and to a Net-RID DP as it does to a Net-RID SP, but its data source must be readily distinguishable via Finders rather than direct from the UAS itself.

7. DRIP Contact

One of the ways in which DRIP can enhance [F3411-22a] with immediately actionable information is by enabling an Observer to instantly initiate secure communications with the UAS remote pilot, Pilot In Command, operator, USS under which the operation is being flown, or other entity potentially able to furnish further information regarding the operation and its intent and/or to immediately influence further conduct or termination of the operation (e.g., land or otherwise exit an airspace volume). Such potentially distracting communications demand strong "AAA" (Authentication, Attestation, Authorization, Access Control, Accounting, Attribution, Audit), per applicable policies (e.g., of the cognizant CAA).

A DRIP entity identifier based on a HHIT, as outlined in Section 3, embeds an identifier of the DIME in which it can be found (expected typically to be the USS under which the UAS is flying), and the procedures outlined in Section 5 enable Observer verification of that relationship. A DRIP entity identifier with suitable records in public and private registries, as outlined in Section 5, can enable lookup not only of information regarding the UAS but also identities of and pointers to information regarding the various associated entities (e.g., the USS under which the UAS is flying an operation), including means of contacting those associated entities (i.e., locators, typically IP addresses).

A suitably equipped Observer could initiate a secure communication channel, using the DET HI, to a similarly equipped and identified entity, i.e., the UA itself, if operating autonomously; the GCS, if the UA is remotely piloted and the necessary records have been populated in the DNS; the USS; etc. Assuming secure communication setup (e.g., via IPsec or HIP), arbitrary standard higher-layer protocols can then be used for Observer to Pilot (O2P) communications (e.g., SIP [RFC3261] et seq), Vehicle to Everything (V2X) (or more specifically Aircraft to Anything (A2X)) communications (e.g., [MAVLink]), etc. Certain preconditions are necessary: 1) each party needs a currently usable means (typically a DNS) of resolving the other party’s DRIP entity identifier to a currently usable locator (IP address), and 2) there must be currently usable bidirectional IP

connectivity (not necessarily via the Internet) between the parties. One method directly supported by the use of HHITs as DRIP entity identifiers is initiation of a HIP Base Exchange (BEX) and Bound End-to-End Tunnel (BEET).

This approach satisfies DRIP requirement GEN-6 Contact, supports satisfaction of DRIP requirements GEN-8, GEN-9, PRIV-2, PRIV-5, and REG-3 [RFC9153], and is compatible with all other DRIP requirements.

8. IANA Considerations

This document has no IANA actions.

9. Security Considerations

The size of the public key hash in the HHIT is vulnerable to a second-preimage attack. It is well within current server array technology to compute another key pair that hashes to the same HHIT (given the current ORCHID construction hash length to fit UAS RID and IPv6 address constraints). Thus, if a receiver were to check HHIT/HI pair validity only by verifying that the received HI and associated information, when hashed in the ORCHID construction, reproduce the received HHIT, an adversary could impersonate a validly registered UA. To defend against this, online receivers should verify the received HHIT and received HI with the HDA (typically USS) with which the HHIT/HI pair purports to be registered. Online and offline receivers can use a chain of received DRIP link endorsements from a root of trust through the RAA and the HDA to the UA, e.g., as described in [DRIP-AUTH] and [DRIP-REGISTRIES].

Compromise of a DIME private key could do widespread harm [DRIP-REGISTRIES]. In particular, it would allow bad actors to impersonate trusted members of said DIME. These risks are in addition to those involving key management practices and will be addressed as part of the DIME process. All DRIP public keys can be found in the DNS, thus they can be revoked in the DNS, and users SHOULD check the DNS when available. Specific key revocation procedures are as yet to be determined.

9.1. Private Key Physical Security

The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. It may be necessary for the GCS to have the key pair to register the HHIT to the USS. Thus, it may be the GCS that generates the key pair and delivers it to the UA, making the GCS a part of the key security boundary. Leakage of the private key, from either the UA or the GCS, to the component manufacturer is a valid concern, and steps need to be in place to ensure safe keeping of the private key. Since it is possible for the UAS RID sender of a small harmless UA (or the entire UA) to be carried by a larger dangerous UA as a "false flag", it is out of scope to deal with secure storage of the private key.

9.2. Quantum Resistant Cryptography

There has been no effort as of yet in DRIP to address post quantum computing cryptography. Small UAS and Broadcast Remote ID communications are so constrained that current post quantum computing cryptography is not applicable. Fortunately, since a UA may use a unique HHIT for each operation, the attack window can be limited to the duration of the operation. One potential future DRIP use for post quantum cryptography is for key pairs that have long usage lives but that rarely, if ever, need to be transmitted over bandwidth constrained links, such as for serial numbers or operators. As the HHIT contains the ID for the cryptographic suite used in its creation, a future post quantum computing safe algorithm that fits

Remote ID constraints may be readily added. This is left for future work.

9.3. Denial-of-Service (DoS) Protection

Remote ID services from the UA use a wireless link in a public space. As such, they are open to many forms of RF jamming. It is trivial for an attacker to stop any UA messages from reaching a wireless receiver. Thus, it is pointless to attempt to provide relief from DoS attacks, as there is always the ultimate RF jamming attack. Also, DoS may be attempted with spoofing/replay attacks; for which, see Section 9.4.

9.4. Spoofing and Replay Protection

As noted in Section 5, spoofing is combatted by the intrinsic self-attesting properties of HHITs, plus their registration. Also, as noted in Section 5, to combat replay attacks, a receiver MUST NOT trust any claims nominally received from an observed UA (not even the Basic ID message purportedly identifying that UA) until the receiver verifies that the private key used to sign those claims is trusted, that the sender actually possesses that key, and that the sender appears indeed to be that observed UA. This requires receiving a complete chain of endorsement links from a root of trust to the UA's leaf DET, plus a message containing suitable nonce-like data signed with the private key corresponding to that DET, and verifying all the foregoing. The term "nonce-like" describes data that is readily available to the prover and the verifier, changes frequently, is not predictable by the prover, and can be checked quickly at low computational cost by the verifier; a Location/Vector message is an obvious choice.

9.5. Timestamps and Time Sources

Section 6 and, more fundamentally, Section 3.3 both require timestamps. In Broadcast RID messages, [F3411-22a] specifies both 32-bit Unix-style UTC timestamps (seconds since midnight going into the 1st day of 2019, rather than 1970) and 16-bit relative timestamps (tenths of seconds since the start of the most recent hour or other specified event). [F3411-22a] requires that 16-bit timestamp accuracy, relative to the time of applicability of the data being timestamped, also be reported, with a worst allowable case of 1.5 seconds. [F3411-22a] does not specify the time source, but GNSS is generally assumed, as latitude, longitude, and geodetic altitude must be reported and most small UAS use GNSS for positioning and navigation.

> | Informative note: For example, to satisfy [FAA_RID], [F3586-22] specifies tamper protection of the entire RID subsystem and use of the GPS operated by the US Government. The GPS has sub-microsecond accuracy and 1.5-second precision. In this example, UA-sourced messages can be assumed to have timestamp accuracy and precision of 1.5 seconds at worst.

GCS often have access to cellular LTE or other time sources better than the foregoing, and such better time sources would be required to support multilateration in Section 6, but such better time sources cannot be assumed generally for purposes of security analysis.

10. Privacy and Transparency Considerations

Broadcast RID messages can contain personal data (Section 3.2 of [RFC6973]), such as the operator ID, and, in most jurisdictions, must contain the pilot/GCS location. The DRIP architectural approach for personal data protection is symmetric encryption of the personal data using a session key known to the UAS and its USS, as follows.

Authorized Observers obtain plaintext in either of two ways: 1) an Observer can send the UAS ID and the cyphertext to a server that offers decryption as a service, and 2) an Observer can send just the UAS ID to a server that returns the session key so that the Observer can directly, locally decrypt all cyphertext sent by that UA during that session (UAS operation). In either case, the server can be a public safety USS, the Observer's own USS, or the UA's USS if the latter can be determined (which, under DRIP, can be from the UAS ID itself). Personal data is protected unless the UAS is otherwise configured, i.e., as part of DRIP-enhanced RID subsystem provisioning, as part of UTM operation authorization, or via subsequent authenticated communications from a cognizant authority. Personal data protection MUST NOT be used if the UAS loses connectivity to its USS; if the UAS loses connectivity, Observers nearby likely also won't have connectivity enabling decryption of the personal data. The UAS always has the option to abort the operation if personal data protection is disallowed, but if this occurs during flight, the UA then MUST broadcast the personal data without protection until it lands and is powered off. Note that normative language was used only minimally in this section, as privacy protection requires refinement of the DRIP architecture and specification of interoperable protocol extensions, which are left for future DRIP documents.

11. References

11.1. Normative References

[F3411-22a] ASTM International, "Standard Specification for Remote ID and Tracking", ASTM F3411-22A, DOI 10.1520/F3411-22A, July 2022, <https://www.astm.org/f3411-22a.html>.

[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>.

[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>.

[RFC9153] Card, S., Ed., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements and Terminology", RFC 9153, DOI 10.17487/RFC9153, February 2022, <https://www.rfc-editor.org/info/rfc9153>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/info/rfc9374>.

11.2. Informative References

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", ANSI/CTA 2063-A, September 2019.

[Delegated] European Union Aviation Safety Agency (EASA), "Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems", March 2019, <https://eur-lex.europa.eu/eli/reg_del/2019/945/oj>.

[DRIP-AUTH]

Wiethuechter, A., Ed., Card, S., and R. Moskowitz, "DRIP Entity Tag Authentication Formats & Protocols for Broadcast Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-auth-30, 28 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-auth-30>.

[DRIP-REGISTRIES]
Wiethuechter, A. and J. Reid, "DRIP Entity Tag (DET) Identity Management Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-registries-12, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-registries-12>.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", ASTM F3411-19, DOI 10.1520/F3411-19, May 2022, <https://www.astm.org/f3411-19.html>.

[F3586-22] ASTM International, "Standard Practice for Remote ID Means of Compliance to Federal Aviation Administration Regulation 14 CFR Part 89", ASTM F3586-22, DOI 10.1520/F3586-22, July 2022, <https://www.astm.org/f3586-22.html>.

[FAA_RID] United States Federal Aviation Administration (FAA), "Remote Identification of Unmanned Aircraft", Federal Register, Vol. 86, No. 10, January 2021, <https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2020-28948.pdf>.

[FAA_UAS_Concept_Of_Ops]
United States Federal Aviation Administration (FAA), "Unmanned Aircraft System (UAS) Traffic Management (UTM) Concept of Operations", v2.0, March 2020, <https://www.faa.gov/sites/faa.gov/files/2022-08/UTM_ConOps_v2.pdf>.

[FS_AEUA] "Study of Further Architecture Enhancement for UAV and UAM", S2-2107092, October 2021, <https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_147E_Electronic_2021-10/Docs/S2-2107092.zip>.

[Implementing]
European Union Aviation Safety Agency (EASA), "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.)", May 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947>.

[Implementing_update]
European Union Aviation Safety Agency (EASA), "Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (Text with EEA relevance)", April 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664>.

[LAANC] United States Federal Aviation Administration (FAA), "Low Altitude Authorization and Notification Capability", <https://www.faa.gov/air_traffic/publications/atpubs/foa_html/chap12_section_9.html>.

[MAVLink] MAVLink, "Micro Air Vehicle Communication Protocol", <http://mavlink.io/>.

[MOC-NOA] United States Federal Aviation Administration (FAA), "Accepted Means of Compliance; Remote Identification of Unmanned Aircraft", Document ID FAA-2022-0859-0001, August 2022, <https://www.regulations.gov/document/FAA-2022-0859-0001>.

[NPA] European Union Aviation Safety Agency (EASA), "Notice of Proposed Amendment 2021-14: Development of acceptable means of compliance and guidance material to support the U-space regulation", December 2021, <https://www.easa.europa.eu/downloads/134303/en>.

[NPRM] United States Federal Aviation Administration (FAA), "Remote Identification of Unmanned Aircraft Systems", Notice of proposed rulemaking, December 2019, <https://www.federalregister.gov/documents/2019/12/31/2019-28100/remote-identification-of-unmanned-aircraft-systems>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7033] Jones, P., Salgueiro, G., Jones, M., and J. Smarr, "WebFinger", RFC 7033, DOI 10.17487/RFC7033, September 2013, <https://www.rfc-editor.org/info/rfc7033>.

[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>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <https://www.rfc-editor.org/info/rfc8004>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <https://www.rfc-editor.org/info/rfc8005>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital

Signature Algorithm (EdDSA)", RFC 8032,
DOI 10.17487/RFC8032, January 2017,
<https://www.rfc-editor.org/info/rfc8032>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

[RFC9224] Blanchet, M., "Finding the Authoritative Registration Data Access Protocol (RDAP) Service", STD 95, RFC 9224, DOI 10.17487/RFC9224, March 2022, <https://www.rfc-editor.org/info/rfc9224>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/info/rfc9334>.

[TR-22.825] 3GPP, "Study on Remote Identification of Unmanned Aerial Systems (UAS)", Release 16, 3GPP TR 22.825, September 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3527>.

[TR-23.755] 3GPP, "Study on application layer support for Unmanned Aerial Systems (UAS)", Release 17, 3GPP TR 23.755, March 2021, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3588>.

[TS-23.255] 3GPP, "Application layer support for Uncrewed Aerial System (UAS); Functional architecture and information flows", Release 17, 3GPP TS 23.255, June 2021, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3843>.

[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 UAS Traffic Management (UTM)

A.1. Operation Concept

The efforts of the National Aeronautics and Space Administration (NASA) and FAA to integrate UAS operations into the national airspace system (NAS) led to the development of the concept of UTM and the ecosystem around it. The UTM concept was initially presented in 2013, and version 2.0 was published in 2020 [FAA_UAS_Concept_Of_Ops].

The eventual concept refinement, initial prototype implementation, and testing were conducted by the joint FAA and NASA UTM research transition team. World efforts took place afterward. The Single European Sky ATM Research (SESAR) started the Concept of Operation for EuROpean UTM Systems (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 their UTM concepts of operations to guide the development of their future air traffic management (ATM) system and ensure safe and efficient integration of manned and unmanned aircraft into the national airspace.

UTM comprises UAS operations infrastructure, procedures, and local regulation compliance policies to guarantee safe UAS integration and operation. The main functionality of UTM includes, but is not limited to, providing 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 UTM has to offer. Such an entity acts as a proxy between UAS operators and UTM service providers. It provides services like real-time UAS traffic monitoring and planning, aeronautical data archiving, airspace and violation control, interacting with other third-party control entities, etc. A USS can coexist with other USS to build a large service coverage map that 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 [LAANC] program, which is the first system to realize some of the envisioned functionality of UTM. The LAANC program can automate UAS operational intent (flight plan) submissions and applications for airspace authorization in real time by checking against multiple aeronautical databases, such as airspace classification and operating rules associated with it, the FAA UAS facility map, special use airspace, Notice to Airmen (NOTAM), and Temporary Flight Restriction (TFR).

A.3. UTM Use Cases for UAS Operations

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

1. For a UAS participating in UTM and taking off or landing in controlled airspace (e.g., Class Bravo, Charlie, Delta, and Echo in the United States), the USS under which the UAS is operating is responsible for verifying UA registration, authenticating the UAS operational intent (flight plan) by checking against a designated UAS facility map database, obtaining the air traffic control (ATC) authorization, and monitoring the UAS flight path in order to maintain safe margins and follow the pre-authorized sequence of authorized 4-D volumes (route).

2. For a UAS participating in UTM and taking off or landing in uncontrolled airspace (e.g., Class Golf in the United States), preflight authorization must be obtained from a USS when operating BVLOS. The USS either accepts or rejects the received operational intent (flight plan) from the UAS. An accepted UAS operation may, and in some cases must, share its current flight data, such as GPS position and altitude, to the USS. The USS may maintain (and provide to authorized requestors) the UAS operation status near real time in the short term and may retain at least some of it in the longer term, e.g., for overall airspace air

traffic monitoring.

Appendix B. Automatic Dependent Surveillance Broadcast (ADS-B)

ADS-B is the de jure technology used in manned aviation for sharing location information, from the aircraft to ground and satellite-based systems, designed in the early 2000s. Broadcast RID is conceptually similar to ADS-B but with the receiver target being the general public on generally available devices (e.g., smartphones).

For numerous technical reasons, ADS-B itself is not suitable for low-flying, small UAS. Technical reasons include, but are not limited to, the following:

1. lack of support for the 1090-MHz ADS-B channel on any consumer handheld devices

2. Cost, Size, Weight, and Power (CSWaP) requirements of ADS-B transponders on CSWaP-constrained UA

3. limited bandwidth of both uplink and downlink, which would likely be saturated by large numbers of UAS, endangering manned aviation

Understanding these technical shortcomings, regulators worldwide have ruled out the use of ADS-B for the small UAS for which UAS RID and DRIP are intended.

Acknowledgments

The work of the FAA’s UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM and 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. Thanks to Alexandre Petrescu, Stephan Wenger, Kyle Rose, Roni Even, Thomas Fossati, Valery Smyslov, Erik Kline, John Scudder, Murray Kucheraway, Robert Wilton, Roman Daniliw, Warren Kumari, Zaheduzzaman Sarker, and Dave Thaler for the reviews and helpful positive comments. Thanks to Laura Welch for her assistance in greatly improving this document. Thanks to Dave Thaler for showing our authors how to leverage the RATS model for attestation in DRIP. Thanks to chairs Daniel Migault and Mohamed Boucadair for direction of our team of authors and editors, some of whom are relative newcomers to writing IETF documents. Thanks especially to Internet Area Director ric Vyncke for guidance and support.

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 (editor)
Intel
2200 Mission College Blvd.
Santa Clara, 95054
United States of America
Email: shuai.zhao@ieee.org

Andrei Gurtov
Linkping University
IDA
SE-58183 Linkping
Sweden
Email: gurtov@acm.org