drip
Internet-Draft
Intended status: Informational
Expires: January 10, 2022

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao (Editor)
Tencent
A. Gurtov
Linkoeping University

July 09, 2021

Drone Remote Identification Protocol (DRIP) Architecture
draft-ietf-drip-arch-14

Abstract

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

Status of This Memo

Copyright Notice

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 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 [I-D.ietf-drip-reqs].

1.1. Overview of Unmanned Aircraft System (UAS) Remote ID (RID) and Standardization

CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

UAS Remote Identification (RID) is an application enabler for a UAS to be identified by Unmanned Aircraft Systems Traffic Management (UTM) and UAS Service Supplier (USS) (Appendix A) or third parties entities such as law enforcement. Many considerations (e.g., safety) dictate that UAS be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. For example, the European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations.

Federal Aviation Administration (FAA)

The FAA published a Notice of Proposed Rule Making [NPRM] in 2019 and whereafter published the "Final Rule" in 2021 [FAA_RID]. In FAA's final rule, it is clearly stated that Automatic Dependent Surveillance Broadcast (ADS-B) Out and transponders can not be used to serve the purpose of an remote identification. More details about ADS-B can be found in Appendix B.

American Society for Testing and Materials (ASTM)

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed the ASTM [F3411-19] Standard Specification for Remote ID and Tracking.

ASTM defines one set of RID information and two means, MAC-layer broadcast and IP-layer network, of communicating it. If an UAS uses both communication methods, the same information must be provided via both means. [F3411-19] is cited by FAA in its RID final rule [FAA_RID] as "a potential means of compliance" to a Remote ID rule.

The 3rd Generation Partnership Project (3GPP)

With release 16, the 3GPP completed the UAS RID requirement study [TS-22.825] and proposed a set of use cases in the mobile network and the services that can be offered based on RID. Release 17 specification focuses on enhanced UAS service requirements and provides the protocol and application architecture support that will be applicable for both 4G and 5G networks.

1.2. Overview of Types of UAS Remote ID

1.2.1. Broadcast RID

A set of RID messages are defined for direct, one-way, broadcast transmissions from the 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.

```
               x x  UA
              xxxxx
                |
                |
                |     app messages directly over
                |     one-way RF data link (no IP)
                |
                |
                +
                x
              xxxxx
                x
                x
                x x   Observer’s device (e.g. smartphone)
              x   x
```

Figure 1

With queries sent over the Internet using harvested RID (see Section 6), the Observer may gain more information about those visible UAS" is only true if the locally observed UAS is (or very recently was) observed somewhere else; harvesting RID is not so much about learning more about directly observed nearby UAS as it is about surveillance of areas too large for local direct visual observation & direct RF link based ID (e.g., an entire air force base, or even larger, a national forest)

1.2.2. Network RID

A RID data dictionary and data flow for Network RID are defined in [F3411-19]. This data flow is emitted from an UAS via unspecified means (but at least in part over the Internet) to a Network Remote ID Service Provider (Net-RID SP). A Net-RID SP provides the RID data to Network Remote ID Display Providers (Net-RID DP). It is the Net-RID DP that responds to queries from Network Remote ID Observers (expected typically, but not specified exclusively, to be web-based) specifying airspace volumes of interest. Network RID depends upon connectivity, in several segments, via the Internet, from the UAS to the Observer.

> Editor-note 1: + list all the segments mentioned above + specify how DRIP provide solutions for each segment

The mimunum Network RID data flow is illustrated in Figure 2:

```
            x x  UA
            xxxxx       ********************
             |   \    *                ------*---+------------+
             |    \   *              /       *  | NET_RID_SP |
             |     \  * ------------/    +---*--+------------+
             | RF   \ */                 |   *
             |        *      INTERNET    |   *  +------------+
             |       /*                  +---*--| NET_RID_DP |
             |      / *                  +---*--+------------+
             +     /   *                 |   *
              x   /     *****************|***      x
            xxxxx                        |       xxxxx
              x                          +-------  x
              x                                    x
             x x   Operator (GCS)      Observer   x x
            x   x                                x   x
```

Figure 2

Command and Control (C2) must flow from the GCS to the UA via some path, currently (in the year of 2021) typically a direct RF link, but with increasing beyond Visual Line of Sight (BVLOS) operations expected often to be wireless links at either end with the Internet between.

> Editor-note 2: Explain the difference with wireless and RF link includes what are the end entities, usages for each transport media.

For all but the simplest hobby aircraft, telemetry (at least position and heading) flows from the UA to the GCS via some path, typically the reverse of the C2 path. Thus, 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.

> Editor-note 3: Does all UAS support telemetry? explain what are simplsest hobby aircraft vs UAS in general. Is it necessary to keep "For all but the simplest hobby aircraft"?

The Net-RID SP forwards RID information via the Internet to subscribed Net-RID DP, typically USS. Subscribed Net-RID DP forward RID information via the Internet to subscribed Observer devices. Regulations require and [F3411-19] describes RID data elements that must be transported end-to-end from the UAS to the subscribed Observer devices.

[F3411-19] prescribes the protocols only between the Net-RID SP, Net-RID DP, and the Discovery and Synchronization Service (DSS). DRIP may also address standardization of protocols between the UA and GCS, between the UAS and the Net-RID SP, and/or between the Net-RID DP and Observer devices.

> Editor-note 4: "DRIP may also..." Specify what protocol DRIP can or will standardize.

> > Informative note: 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 RID information is in the scope of [F3411-19] Network RID.

1.3. Overview of USS Interoperability

With Net-RID, there is direct communication between the UAS and its USS. With Broadcast-RID, the UAS Operator has either pre-filed a 4D space volume for USS operational knowledge and/or Observers can be providing information about observed UA to a USS. USS exchange information via a Discovery and Synchronization Service (DSS) so all

USS collectively have knowledge about all activities in a 4D airspace.

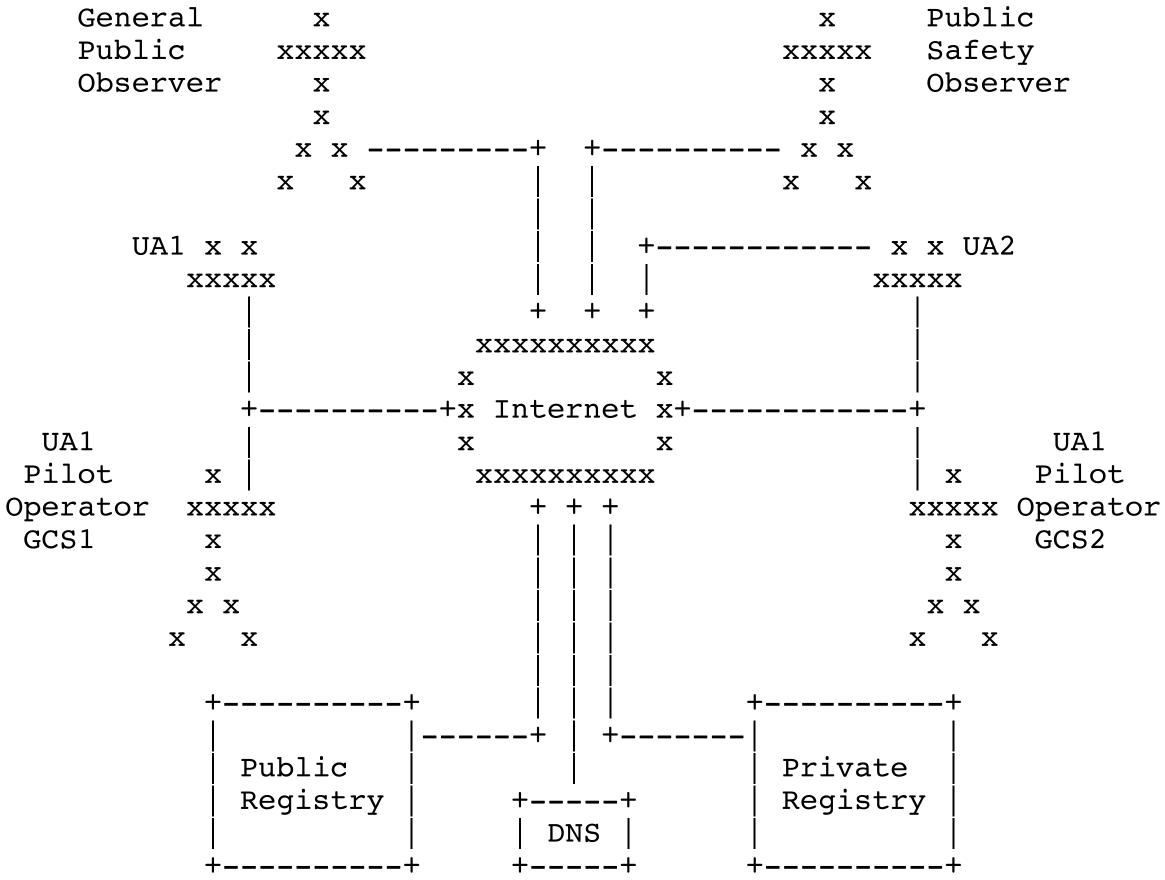
The interactions among Observer, UA, and USS are shown in Figure 3.

```
                               +----------+
                               | Observer |
                               +----------+
                              /            \
                             /              \
                      +-----+                +-----+
                      | UAS1 |                | UAS2 |
                      +-----+                +-----+
                             \              /
                              \            /
                               +----------+
                               | Internet |
                               +----------+
                              /            \
                             /              \
                       +-------+           +-------+
                       | USS1 | <-------> | USS2 |
                       +-------+           +-------+
                                \         /
                                 \       /
                                 +------+
                                 |  DSS |
                                 +------+
```

Figure 3

1.4. Overview of DRIP Architecture

The requirements document [I-D.ietf-drip-reqs] provides an extended introduction to the problem space and use cases. Only a brief summary of that introduction is restated here as context, with reference to the general UAS RID usage scenarios shown in Figure 4.



```
         General      x                           x     Public
         Public     xxxxx                       xxxxx   Safety
         Observer     x                           x     Observer
                      x                           x
                     x x ---------+  +---------- x x
                    x   x         |  |          x   x
                                  |  |
            UA1 x x               |  |  +------------ x x UA2
               xxxxx              |  |  |            xxxxx
                  |               +  +  +              |
                  |            xxxxxxxxxx              |
                  |           x          x             |
                  +----------+x Internet x+------------+
       UA1        |           x          x             |       UA1
      Pilot     x |            xxxxxxxxxx              | x    Pilot
     Operator  xxxxx              + + +                xxxxx Operator
      GCS1      x                 | | |                  x    GCS2
                x                 | | |                  x
               x x                | | |                 x x
              x   x               | | |                x   x
                                  | | |
                +----------+      | | |       +----------+
                |          |------+ | +-------|          |
                | Public   |        |         | Private  |
                | Registry |     +-----+      | Registry |
                |          |     | DNS |      |          |
                +----------+     +-----+      +----------+
```

Figure 4

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 [F3411-19] and other external standards, to satisfy UAS RID requirements.

This document outlines the UAS RID architecture. This includes presenting the gaps between the CAAs' Concepts of Operations and [F3411-19] as it relates to the use of Internet technologies and UA direct RF communications. Issues include, but are not limited to:

- Design of trustworthy remote ID and trust in RID messages (Section 4)

- Mechanisms to leverage Domain Name System (including DNS: [RFC1034]), Extensible Provisioning Protocol (EPP [RFC5731]) and Registration Data Access Protocol (RDAP) ([RFC7482]) for publishing public and private information (see Section 5.1 and Section 5.2).

- Harvesting broadcast RID messages for UTM inclusion (Section 6).

- Privacy in RID messages (PII protection) (Section 9).

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown above.

3. Definitions and Abbreviations

Editor-note 13: 1) should we merge Section 2 and Section 3 2) how should we list abbr in the Arch? Previous WG agreement is that all the DRIP terms shall be defined in -reqs, which may or may not be used in -reqs itself, but other documents such as Arch-. And arch- can list terms when they are used in the arch- only. So which is which ?

3.1. Additional Definitions

This document uses terms defined in [I-D.ietf-drip-reqs].

3.2. Abbreviations

ADS-B:	Automatic Dependent Surveillance Broadcast
DSS:	Discovery & Synchronization Service
EdDSA:	Edwards-Curve Digital Signature Algorithm
GCS:	Ground Control Station
HHIT:	Hierarchical HIT Registries

HIP:	Host Identity Protocol
HIT:	Host Identity Tag
RID:	Remote ID
Net-RID SP:	Network RID Service Provider
Net-RID DP:	Network RID Display Provider.
PII:	Personally Identifiable Information
RF:	Radio Frequency
SDSP:	Supplemental Data Service Provider
UA:	Unmanned Aircraft
UAS:	Unmanned Aircraft System
USS:	UAS Service Supplier
UTM:	UAS Traffic Management

3.3. Claims, Assertions, Attestations, and Certificates

This section introduces the terms "Claims", "Assertions", "Attestations", and "Certificates" as used in DRIP. DRIP certificate has a different context compared with security certificates and Public Key Infrastructure used in X.509.

Editor-note 5: To be confirmed

Claims:

A claim in DRIP is a predicate (e.g., "X is Y", "X has property Y", and most importantly "X owns Y" or "X is owned by Y").

Assertions:

An assertion in DRIP is a set of claims. This definition is borrowed from JWT [RFC7519] and CWT [RFC8392].

Attestations:

An attestation in DRIP is a signed assertion. The signer may be a claimant or a third party. Under DRIP this is normally used when an entity asserts a relationship with another entity, along with other information, and the asserting entity signs the assertion, thereby making it an attestation.

Certificates:

A certificate in DRIP is an attestation, strictly over identity information, signed by a third party.

4. HHIT as the Primary DRIP Entity Identifier

This section describes the DRIP architectural approach to meeting the basic requirements of a DRIP entity identifier within external technical standard ASTM [F3411-19] and regulatory constraints. It justifies and explains the use of Hierarchical Host Identity Tags (HHITs) as self-asserting IPv6 addresses suitable as a UAS ID type and more generally as trustworthy multipurpose remote identifiers.

A HHIT, together with the Host Identity (HI) from which it is partly derived, self-attests to its included explicit registration hierarchy, providing Registrar discovery for a 3rd-party who is looking for ID attestation retrieves the necessary information to the registrar via a DNS request HHIT.

Editor-note 6: Is there a need to specify how self-attest works? if yes then where? possible a new section under Section 4}

4.1. UAS Remote Identifiers Problem Space

Editor-note 14: Good to have: adding match requirment numbering from requirement document

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

The Broadcast RID data exchange faces extreme challenges due to the limitation of the demanding support for Bluetooth. The ASTM [F3411-19] defines the basic RID message which is expected to contain certain RID data and the Authentication message. The Basic RID message has a maximum payload of 25 bytes and the maximum size allocated by ASTM for the RID is 20 bytes and only 3 bytes are left unused. currently, the authentication maximum payload is defined to be 201 bytes.

> Editor-note 7: To be more specific about the RID message header and payload structure, such as 1) list different type of BRID messages defined in ASTM F3411, 2) how many bytes for each filed.

Standard approaches like X.509 and PKI will not fit these constraints, even using the new EdDSA [RFC8032] algorithm cannot fit within the maximum 201 byte limit, due in large measure to ASN.1 encoding format overhead.

An example of a technology that will fit within these limitations is an enhancement of the Host Identity Tag (HIT) of HIPv2 [RFC7401] using Hierarchical HITs (HHITs) for UAS RID [I-D.ietf-drip-rid]. As PKI with X.509 is being used in other systems with which UAS RID must interoperate (e.g. Discovery and Synchronization Service and any other communications involving USS) mappings between the more flexible but larger X.509 certificates and the HHIT-based structures can must be devised. This could be as in [RFC8002] or simply the HHIT as Subject Alternative Name (SAN) and no Distinguished Name (DN).

> Editor-note 8: is there a need to explain the how binding/proxy/ translation between the HHIT and X509? Should this be addressed in Arch- or solution?

A self-attestation of the HHIT RID can be done in as little as 84 bytes, by avoiding an explicit encoding technology like ASN.1 or Concise Binary Object Representation (CBOR [RFC8949]). This compressed attestation consists of only the HHIT, a timestamp, and the EdDSA signature on them.

> Editor-note 9: to be more specific regarding how HHIT can only use as little as 84 bytes to address the crypto concern.

The HHIT prefix and suiteID provide crypto agility and implicit encoding rules. Similarly, a self-attestation of the Hierarchical registration of the RID (an attestation of a RID third-party registration "certificate") can be done in 200 bytes. Both these are detailed in UAS RID [I-D.ietf-drip-rid].

> Editor-note 10: to be more specific why 200 bytes is sufficient.

An Observer would need Internet access to validate a self-attestations claim. A third-party Certificate can be validated via a small credential cache in a disconnected environment. This third-party Certificate is possible when the third-party also uses HHITs for its identity and the UA has the public key and the Certificate for that HHIT.

4.2. HIT as A Trustworthy DRIP Entity Identifier

Editor-note 15: general comments about rewrite of this section due to lack of coherence.

A Remote ID that can be trustworthily used in the RID Broadcast mode can be built from an asymmetric keypair. Rather than using a key signing operation to claim ownership of an ID that does not guarantee name uniqueness, in this method the ID is cryptographically derived directly from the public key. The proof of ID ownership (verifiable attestation, versus mere claim) is guaranteed by signing this cryptographic ID with the associated private key. The association between the ID and the private key is ensured by cryptographically binding the public key with the ID, more specifically the ID results from the hash of the public key. It is statistically hard for another entity to create a public key that would generate (spoof) the ID.

The HITs is designed statistically unique through the cryptographic hash feature of second-preimage resistance. The cryptographically-bound addition of the Hierarchy and an HHIT registration process (e.g. based on Extensible Provisioning Protocol, [RFC5730]) 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 UUID or device serial number) as the subject in an X.509 certificate.

Editor-note 11: Explain how HIT itself and HHIT registry address naming collision.

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 can 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 (more details in Section 8).

In another case, a UAS equipped for Broadcast RID can 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 Network RID can be provisioned likewise; the private key resides 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 can be provisioned either with public keys of the DRIP identifier root registries or certificates for subordinate registries.

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

4.3. HHIT for DRIP Identifier Registration and Lookup

Remote ID 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 Remote ID itself needs to be the inquiry input into the lookup. An HHIT DRIP identifier contains cryptographically embedded registration information. This HHIT registration hierarchy, along with the IPv6 prefix, is trustable and sufficient information that can be used to perform such a lookup. Additionally, the IPv6 prefix can enhance the HHITs use beyond the basic Remote ID function (e.g use in HIP, [RFC7401]).

> Editor-note 12: more description regarding 1) Is that something we should address in the Arch- 2) if yes, then adding more text about how a trustable lookup is performed

Therefore, a DRIP identifier can be represented as a HHIT. It can be self-generated by a UAS (either UA or GCS) and registered with the Private Information Registry (More details in Section 5.2) identified in its hierarchy fields. Each DRIP identifier represented as an HHIT can not be used more than once.

4.4. HHIT for DRIP Identifier Cryptographic

The only (known to the authors of this document at the time of its writing) extant fixed-length ID cryptographically derived from a public key are the Host Identity Tag [RFC7401], HITs, and Cryptographically Generated Addresses [RFC3972], CGAs. However, both HITs and CGAs lack registration/retrieval capability. HHIT, on the other hand, is capable of providing a cryptographic hashing function, along with a registration process to mitigate the probability of a hash collision (first registered, first allowed).

5. DRIP Identifier Registration and Registries

> Editor-note 16: Fundamentally disagree with not actually specifying an architecture in the DRIP Architecture document (From Stuart Card)

UAS registries can hold both public and private UAS information 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. A DRIP identifier is amenable to handling as an Internet domain name (at an arbitrary level in the hierarchy). It also can be registered in at least a pseudo-domain (e.g. .ip6.arpa for reverse lookup), or as a sub-domain (for forward lookup). This section introduces the public and private information registries for DRIP identifiers.

5.1. Public Information Registry

5.1.1. Background

The public registry provides trustable information such as attestations of RID ownership and HDA registration. Optionally, pointers to the repositories for the HDA and RAA implicit in the RID can be included (e.g. for HDA and RAA HHIT|HI used in attestation signing operations). This public information will be principally used by Observers of Broadcast RID messages. Data on UAS that only use Network RID, is only available via an Observer's Net-RID DP that would tend to provide all public registry information directly. The Observer can visually "see" these UAS, but they are silent to the Observer; the Net-RID DP is the only source of information based on a query for an airspace volume.

5.1.2. Proposed Approach

A DRIP public information registry can respond to standard DNS queries, in the definitive public Internet DNS hierarchy. If a DRIP public information registry lists, in a HIP RR, any HIP RVS servers for a given DRIP identifier, those RVS servers can restrict relay services per AAA policy; this requires extensions to [RFC8004]. These public information registries can use secure DNS transport (e.g. DNS over TLS) to deliver public information that is not inherently trustable (e.g. everything other than attestations).

5.2. Private Information Registry

5.2.1. 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: 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 a USS, and likely integrated with a USS.

5.2.2. Proposed Approach

A DRIP private information registry can support essential Internet domain name registry operations (e.g. add, delete, update, query) using interoperable open standard protocols. It can also support the Extensible Provisioning Protocol (EPP) and the Registry Data Access Protocol (RDAP) with access controls. It might be listed in a DNS: that DNS could be private; but absent any compelling reasons for use of private DNS, a public DNS hierarchy needs to be in place. 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 [RFC7484]. A DRIP private information registry can also support WebFinger as specified in [RFC7033].

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 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 also considering Network RID. The FAA RID Final Rules [FAA_RID] only specify Broadcast RID for UAS, however, still encourages Network RID for complementary functionality, especially in support of UTM.

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. It offers considerable enhancement over some Network RID options such as only reporting planned 4D operation space by the operator.

These gateways could be pre-positioned (e.g. around airports, public gatherings, and other sensitive areas) and/or crowd-sourced (as nothing more than a smartphone with a suitable app is needed). As Broadcast RID media have limited range, gateways receiving messages claiming locations far from the gateway can alert authorities or a SDSP to the failed sanity check possibly indicating intent to deceive. Surveillance SDSPs can use messages with precise date/time/position stamps from the gateways to multilaterate UA location, independent of the locations claimed in the messages (which may have a natural time lag as it is), which are entirely operator self-reported in UAS RID and UTM, and thus are subject not only to natural time lag and error but also operator misconfiguration or intentional deception.

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 RID messages. This Crowd Sourced Remote ID (CS-RID) would be a significant enhancement, beyond baseline DRIP functionality; if implemented, it adds two more entity types.

6.1. The CS-RID Finder

A CS-RID Finder is the gateway for Broadcast Remote ID Messages into the 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 Network RID client. It would 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.

6.2. The CS-RID SDSP

A CS-RID SDSP would 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. A CS-RID SDSP should appear (i.e. present the same interface) to a Net-RID SP as a Net-RID DP.

7. IANA Consideration

This document does not make any IANA request.

8. Security Considerations

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. Keys may be extracted from a GCS or UA. The RID sender of a small harmless UA (or the entire UA) could be carried by a larger dangerous UA as a "false flag." 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.

9. Privacy & Transparency Considerations

Broadcast RID messages can contain PII. A viable architecture for PII protection would be symmetric encryption of the PII using a session key known to the UAS and its USS. An authorized Observer could send the encrypted PII along with the UAS ID (to the USS in which the UAS ID is registered if that can be determined, e.g., from received Broadcast RID information such as the UAS ID itself, or to the Observer's USS, or to a Public Safety USS) to get the plaintext. Alternatively, the authorized Observer can receive the key to directly decrypt all PII content sent by that UA during that session (UAS operation).

An authorized Observer can instruct a UAS via the USS that conditions have changed mandating no PII protection or land the UA (abort the operation).

PII can be protected unless the UAS is informed otherwise. This could come as part of UTM operation authorization. It can be special instructions at the start or during an operation. PII protection can not be used if the UAS loses connectivity to the USS. The UAS always has the option to abort the operation if PII protection is disallowed.

10. References

10.1. Normative References

[I-D.ietf-drip-reqs]
Card, S. W., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", draft-ietf-drip-reqs-17 (work in progress), July 2021.

[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>.

10.2. Informative References

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

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

[FAA_RID] United States Federal Aviation Administration (FAA), "Remote Identification of Unmanned Aircraft", 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)", 2020, <https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf>.

[I-D.ietf-drip-rid]
Moskowitz, R., Card, S. W., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", draft-ietf-drip-rid-07 (work in progress), January 2021.

[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", 2019.

[LAANC] United States Federal Aviation Administration (FAA), "Low Altitude Authorization and Notification Capability", n.d., <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", 2019.

[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>.

[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>.

[RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, DOI 10.17487/RFC5731, August 2009, <https://www.rfc-editor.org/info/rfc5731>.

[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>.

[RFC7482] Newton, A. and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format", RFC 7482, DOI 10.17487/RFC7482, March 2015, <https://www.rfc-editor.org/info/rfc7482>.

[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>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8002] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 8002, DOI 10.17487/RFC8002, October 2016, <https://www.rfc-editor.org/info/rfc8002>.

[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>.

[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>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

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

[U-Space] European Organization for the Safety of Air Navigation (EUROCONTROL), "U-space Concept of Operations", 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 FAA's effort of integrating UAS's operation 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 UTM research transition team 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 ensure safe and efficient integrations of manned and unmanned aircraft into the national airspace.

The UTM comprises UAS operation infrastructure, procedures and local regulation compliance policies to guarantee safe UAS integration and operation. The main functionality of a 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 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 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 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 [LAANC] program which is the first system to realize some of the UTM envisioned functionality. The LAANC program can automate the UAS’s flight 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 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 a 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 designated UAS fly map database, obtaining the air traffic control (ATC) authorization and monitor 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 an uncontrolled airspace (ex. Class Golf in the United States), pre-flight authorization must be obtained from a USS when operating beyond-visual-of-sight (BVLOS). The USS either accepts or rejects received operational intent (flight plan) from the UAS. Accepted UAS operation may share its current flight data such as GPS position and altitude to USS. The USS may keep the UAS operation status near real-time and may keep it as a record for overall airspace air traffic monitoring.

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

The 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 UA. Technical reasons include but not limited to the following:

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

2. Weight and cost 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.

Acknowledgements

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. IETF volunteers who have contributed to this draft include Amelia Andersdotter and Mohamed Boucadair.

Authors' Addresses

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
USA

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
USA

Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
USA

Email: rgm@labs.htt-consult.com

Shuai Zhao
Tencent
2747 Park Blvd
Palo Alto 94588
USA

Email: shuai.zhao@ieee.org

Andrei Gurtov
Linkoeping University
IDA
Linkoeping SE-58183 Linkoeping
Sweden

Email: gurtov@acm.org