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

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 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]. The requirements document provides an extended introduction to the problem space and use cases.

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

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

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 clearly states that Automatic Dependent Surveillance Broadcast (ADS-B) Out and transponders cannot be used to satisfy the RID requirements on UAS to which the rule applies (see Appendix B).

European Union Aviation Safety Agency (EASA)

The EASA published a [Delegated] regulation in 2019 imposing requirements on UAS manufacturers and third-country operators, including but not limited to RID requirements. The EASA also published in 2019 an [Implementing] regulation laying down detailed rules and procedures for UAS operations and operating personnel.

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] 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] 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. The study of Further Architecture Enhancement for Uncrewed Aerial Vehicles (UAV) and Urban Air Mobility (UAM) [FS_AEUA] in release 18 further enhances the communication mechanism between UAS and USS/ UTM. The RID discussed in Section 4 may be used as the 3GPP CAA-level ID for Remote Identification purposes.

1.2. Overview of Types of UAS Remote ID

1.2.1. Broadcast RID

[F3411] defines a set of RID messages 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.

```
            +------------------------+
            | Unmanned Aircraft (UA) |
            +-----------o------------+
                        |
                        |
                        |
                        | app messages directly over
                        | one-way RF data link (no IP)
                        |
                        |
                        v
        +------------------o-------------------+
        | Observer's device (e.g., smartphone) |
        +--------------------------------------+
```
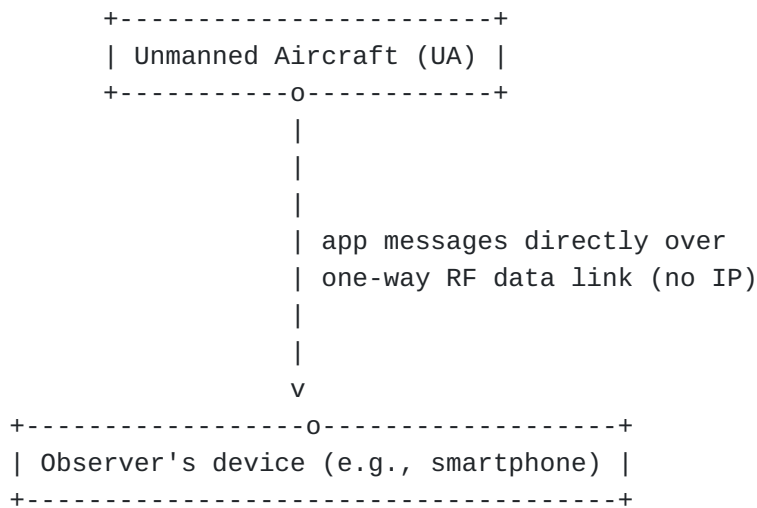
                           Figure 1

   Broadcast RID provides information only about unmanned aircraft (UA)
   within direct RF LOS, typically similar to visual Line-Of-Sight
   (LOS), 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 ID (see Section 7).

1.2.2. Network RID

   [F3411], 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 RID is generated by the UAS,
      typically some by the UA and some by the GCS (Ground Control
      Station), e.g. their respective GNSS derived locations.

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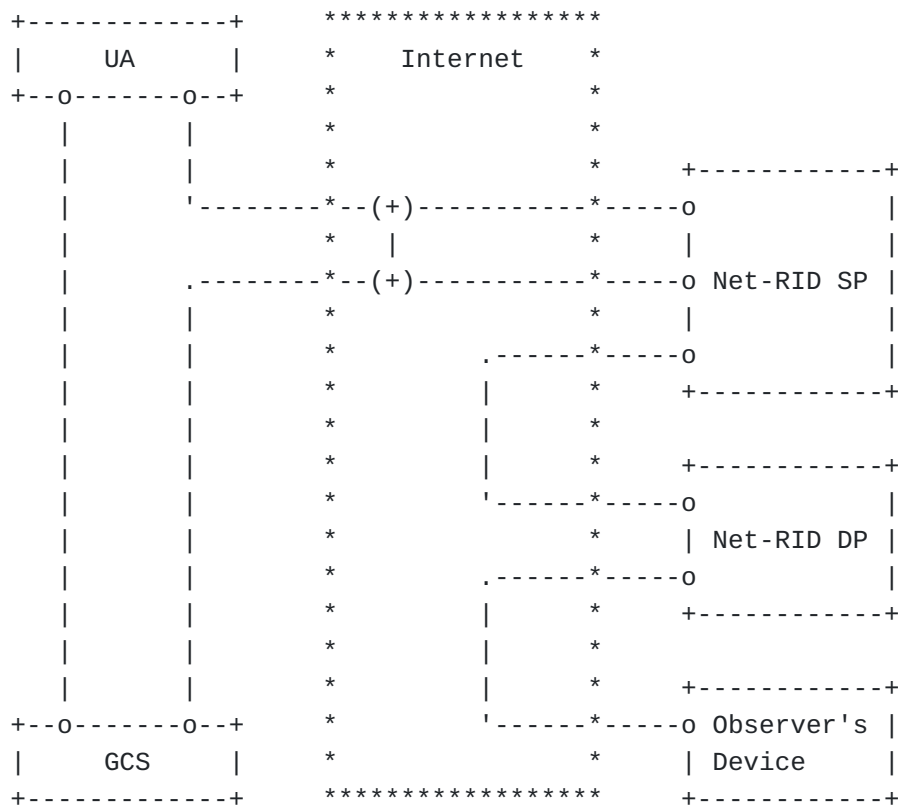
     *An Observer's device, expected typically but not specified to be
      web based, queries a Network Remote Identification Display
      Provider (Net-RID DP), typically also a USS, about any operations
      in a specific 4-D airspace volume.
```

*Using fully specified web based methods over the Internet, the
    Net-RID DP queries all Net-RID SP 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 SP and responds to the Observer's query.

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

```
+-------------+     *****************
|     UA      |     *    Internet    *
+--o-------o--+     *                 *
   |       |        *                 *
   |       |        *                 *      +------------+
   |       '--------*--(+)-----------*-----o             |
   |       |        *   |            *     |             |
   |       .--------*--(+)-----------*-----o Net-RID SP  |
   |       |        *                 *    |             |
   |       |        *       .------*-----o             |
   |       |        *       |        *     +------------+
   |       |        *       |        *
   |       |        *       |        *     +------------+
   |       |        *       '------*-----o             |
   |       |        *                 *    | Net-RID DP  |
   |       |        *       .------*-----o             |
   |       |        *       |        *     +------------+
   |       |        *       |        *
   |       |        *       |        *     +------------+
+--o-------o--+     *       '------*-----o Observer's  |
|     GCS     |     *                 *    | Device     |
+------------+     *****************      +------------+
```


                              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,
   it is expected often to be wireless links at either end with the
   Internet between.

   Telemetry (at least UA's 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.

   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] describes RID data elements that
must be transported end-to-end from the UAS to the subscribed
Observer devices.

[F3411] prescribes the protocols between the Net-RID SP, Net-RID DP,
and the DSS. It also prescribes data elements (in JSON) between
Observer and Net-RID DP. DRIP could address standardization of
secure protocols between the UA and 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.

> 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] Network RID.

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 4D
airspace. The interactions among an Observer, multiple UAS, and
their USS are shown in Figure 3.

```
        +------+     +----------+    +------+
        | UAS1 |     | Observer |    | UAS2 |
        +---o--+     +-----o----+    +--o---+
            |              |             |
     ******|************* |*************|******
     *      |             |             |     *
     *      |         +---o--+          |     *
     *      |  .------o USS3 o------.    |     *
     *      | |       +--o---+      | |  *
     *      | |          |          | |  *
     *    +-o--o-+    +--o--+     +-o--o-+  *
     *    |       o----o DSS o-----o      |  *
     *    | USS1 |    +-----+       | USS2 |  *
     *    |       o---------------o       |  *
     *    +------+                  +------+  *
     *                                       *
     *                Internet               *
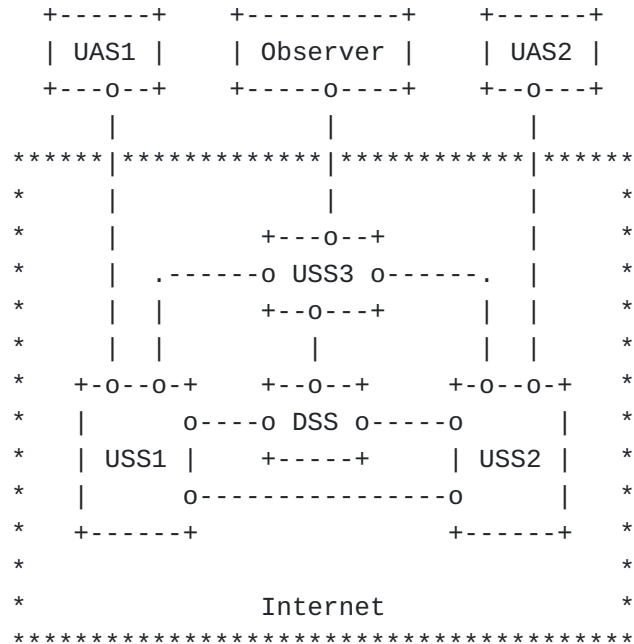     *****************************************
```

Figure 3

1.4. Overview of DRIP Architecture

Figure 4 illustrates the general 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 (2022) chartered).

```
***************                                    ***************
*    UAS1      *                                   *    UAS2     *
*             *                                    *             *
* +--------+  *                 DAA/V2V            *  +--------+ *
* |  UA   o--*-----------------------------------*--o   UA   | *
* +--o--o--+  *                                   *  +--o--o--+ *
*    | |      *   +------+    Lookups    +------+  *     | |    *
*    | |      *   | GPOD o------.   .------o PSOD |  *   | |    *
*    | |      *   +------+      |   |     +------+  *   | |    *
*    | |      *                 |   |              *     | |    *
* C2 | |      *     V2I    ************    V2I     *     | | C2 *
*    |  '-----*-------------*        *-------------*-----'  |   *
*    |        *             *        *             *        |   *
*    |        o====Net-RID===*       *====Net-RID===o       |   *
* +--o--+     *              * Internet *            *     +--o--+ *
* | GCS o-----*-------------*          *-------------*-----o GCS | *
* +-----+     * Registration *         * Registration *   +-----+ *
*            * (and UTM)    *          * (and UTM)    *          *
***************             ************              ***************
                        |   |   |
           +----------+  |   |   |   +----------+
           | Public   o---'  |   '---o Private  |
           | Registry |      |       | Registry |
           +----------+      |       +----------+
                          +--o--+
                          | DNS |
                          +-----+
```

GPOD: General Public Observer Device (for brevity in this figure)
PSOD: Public Safety Observer Device (for brevity in this figure)

                            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] 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 presenting the gaps between the
   CAAs' Concepts of Operations and [F3411] 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 identifiers ([Section 4](#)).

  -Mechanisms to leverage Domain Name System (DNS [RFC1034]),
   Extensible Provisioning Protocol (EPP [RFC5731]) and
   Registration Data Access Protocol (RDAP) ([RFC9082]) for
   publishing public and private information (see [Section 5.1](#) and
   [Section 5.2](#)).

  -Specific authentication methods and message payload formats to
   enable verification that Broadcast RID messages were sent by
   the claimed sender ([Section 6](#)) and that sender is in the
   claimed registry ([Section 5](#) and [Section 6](#)).

  -Harvesting broadcast RID messages for UTM inclusion ([Section 7](#)).

  -Methods for instantly establishing secure communications
   between an Observer and the pilot of an observed UAS ([Section 8](#)).

  -Privacy in RID messages (PII protection) ([Section 11](#)).

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 here.

3. Terms and Definitions

3.1. Abbreviations

EdDSA: Edwards-Curve Digital Signature Algorithm

HHIT: Hierarchical HIT

HIP: Host Identity Protocol

HIT: Host Identity Tag

3.2. 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.

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
   the claimant or a related party with stake in the assertion(s).
   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. This third party should be
   one with no stake in the attestation(s) over which it is signing.

3.3. Additional Definitions

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

4. HHIT as the 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] 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.

   Self-asserting in this usage is given by the Host Identity (HI), the
   HHIT ORCHID construction and a signature of the HHIT by the HI can
   both be validated. The explicit registration hierarchy within the
   HHIT provides registry discovery (managed by a Registrar) to either
   yield the HI for 3rd-party (who is looking for ID attestation)
   validation or prove the HHIT and HI have uniquely been registered.

4.1. UAS Remote Identifiers Problem Space

A DRIP entity identifier needs to be "Trustworthy" (See DRIP
Requirement GEN-1, ID-4 and ID-5 in [I-D.ietf-drip-reqs]). This
means that given a sufficient collection of 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 Requirements GEN-3 and ID-2).

Broadcast RID, especially its support for Bluetooth 4, imposes
severe constraints. ASTM RID [F3411] allows a UAS ID of types 1, 2
and 3 of 20 bytes; a revision to [F3411], currently in balloting (as
of Oct 2021), adds type 4, Specific Session ID, to be standardized
by IETF and other standard development organizations (SDOs) as
extensions to ASTM RID, consumes one of those bytes to index the
sub-type, leaving only 19 for the identifier (see DRIP Requirement
ID-1).

Likewise, the maximum ASTM RID [F3411] Authentication Message
payload is 201 bytes for most authentication types, but for type 5,
also added in this revision, for IETF and other SDOs to develop
Specific Authentication Methods as extensions to ASTM RID, one byte
is consumed to index the sub-type, leaving only 200 for DRIP
authentication payloads, including one or more DRIP entity
identifiers and associated authentication data.

4.2. HHIT as A Trustworthy DRIP Entity Identifier

A Remote ID that can be trustworthily used in the RID Broadcast mode
can be built from an asymmetric keypair. 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.
The public key is designated as the HI while the ID is designated as
the HIT.

By construction, the HIT is statistically unique through the
cryptographic hash feature of second-preimage resistance. The
cryptographically-bound addition of the Hierarchy and an 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 UUID or device serial number) as the
subject in an X.509 certificate.

A UA equipped for Broadcast RID SHOULD 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 SHOULD 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 SHOULD 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.

A self-attestation of a HHIT used as a UAS ID can be done in as little as 84 bytes when Ed25519 [RFC8032] is used, by avoiding an explicit encoding technology like ASN.1 or Concise Binary Object Representation (CBOR [RFC8949]). This attestation consists of only the HHIT, a timestamp, and the EdDSA signature on them.

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 (more details in Section 10).

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

4.3. HHIT for DRIP Identifier Registration and Lookup

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. This is the defense against a cryptographic hash second pre-image attack on the HHIT (e.g. multiple HIs yielding the same HHIT, see Requirement

ID-3). A lookup of the HHIT into this registration data provides the registered HI for HHIT proof of ownership. A first-come-first-serve registration for a HHIT provides deterministic access to any other needed actionable information based on inquiry access authority (more details in Section 5.2).

4.4. HHIT as a Cryptographic Identifier

The only (known to the authors at the time of this writing) extant 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 and a cryptographic hash of that information concatenated with the entity's public key, etc. Although hash collisions may occur, the registrar can detect them and reject registration requests rather than issue credentials, e.g., by enforcing a first-claimed, first-attested policy. Pre-image hash attacks are also mitigated through this registration process, locking the HHIT to a specific HI

5. DRIP Identifier Registration and Registries

DRIP registries 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. This section introduces the public and private information registries for DRIP identifiers. This DRIP Identifier registration process satisfies the following DRIP requirements defined in [I-D.ietf-drip-reqs]: GEN-3, GEN-4, ID-2, ID-4, ID-6, PRIV-3, PRIV-4, REG-1, REG-2, REG-3 and REG-4.

5.1. Public Information Registry

5.1.1. Background

The public registry provides trustable information such as attestations of RID ownership and registration with the HDA (Hierarchical HIT Domain Authority). Optionally, pointers to the registries for the HDA and RAA (Registered Assigning Authority)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 available via an Observer's Net-RID DP that would tend to directly provide all public registry information. The Observer may visually "see" these Net-RID

UAS, but they may be 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. DNS as the Public DRIP Identifier Registry

A DRIP identifier SHOULD be registered as an Internet domain name (at an arbitrary level in the hierarchy, e.g. in .ip6.arpa). Thus DNS can provide all the needed public DRIP information. A standardized HHIT FQDN (Fully Qualified Domain Name) can deliver the HI via a HIP RR (Resource Record) [RFC8005] and other public information (e.g., RRA and HDA PTRs, and HIP RVS (Rendezvous Servers) [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. The HHIT hierarchy can provide the needed scalability and management structure. 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. The lookup function may be implemented by the Net-RID DPs.

5.2.2. EPP and RDAP as the Private DRIP Identifier Registry

A DRIP private information registry supports essential registry operations (e.g. add, delete, update, query) using interoperable open standard protocols. It can accomplish this by using 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 [RFC7484].

5.2.3. 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 deployed. These alternative methods may be used by Net-RID DP with specific customers.

6. DRIP Identifier Trust

While the DRIP entity identifier is self-asserting, it alone does not provide the "trustworthiness" specified in [I-D.ietf-drip-reqs]. For that it MUST be registered (under DRIP Registries) and be actively used by the party (in most cases the UA). A sender's identity can not be approved by only possessing a DET (DRIP Entity Tag which is an HHIT-based UA ID) and broadcasting a claim that it belongs to that sender. Even the sender using that HI's private key to sign static data proves nothing as well, as it is subject to trivial replay attacks. Only sending the DET and a signature on frequently changing data that can be sanity checked by the Observer (such as a Location/Vector message) proves that the observed UA possesses the claimed UAS ID.

For Broadcast RID, this is a challenge to balance the original requirements of Broadcast RID and the efforts needed to satisfy the DRIP requirements all under severe constraints. 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.

An optimization of different DRIP Authentication Messages allows an Observer, without Internet connection (offline) or with (online), to be able to validate a UAS DRIP ID in real-time. First is the sending of Broadcast Attestations (over DRIP Link Authentication Messages) [I-D.ietf-drip-auth] containing the relevant registration of the UA's DRIP ID in the claimed Registry. Next is sending DRIP Wrapper Authentication Messages that sign over both static (e.g. above registration) and dynamically changing data (such as UA location data). Combining these two sets of information an Observer can piece together a chain of trust and real-time evidence to make their determination of the UAs claims.

This process (combining the DRIP entity identifier, Registries and Authentication Formats for Broadcast RID) can satisfy the following DRIP requirement defined in [I-D.ietf-drip-reqs]: GEN-1, GEN-2, GEN-3, ID-2, ID-3, ID-4 and ID-5.

7. 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] permit only Broadcast RID for rule

compliance, but still encourage 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 advantages over either form of RID alone: greater fidelity than Network RID reporting of planned area operations; surveillance of areas too large for local direct visual observation and direct 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 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 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.

This approach satisfies the following DRIP requirements defined in [I-D.ietf-drip-reqs]: GEN-5, GEN-11, and REG-1.

7.1. 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, similar to but readily distinguishable from that between a GCS and a Net-RID SP.

7.2. The CS-RID SDSP

A CS-RID SDSP aggregates and processes (e.g., estimates UA location using multilateration when possible) information collected by CS-RID Finders. A CS-RID SDSP should appear (i.e. present the same interface) to a Net-RID SP as a Net-RID DP.

8. DRIP Contact

One of the ways in which DRIP can enhance [F3411] 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 4
embeds an identifier of the registry in which it can be found
(expected typically to be the USS under which the UAS is flying) and
the procedures outlined in Section 6 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). An Observer equipped with HIP can
initiate a Base Exchange (BEX) and establish a Bound End to End
Tunnel (BEET) protected by IPsec Encapsulating Security Payload
(ESP) encryption to a likewise equipped and identified entity: the
UA itself, if operating autonomously; the GCS, if the UA is remotely
piloted and the necessary records have been populated in DNS;
likewise the USS, etc. Certain preconditions are necessary: each
party to the communication needs a currently usable means (typically
DNS) of resolving the other party's DRIP entity identifier to a
currently usable locator (IP address); and there must be currently
usable bidirectional IP (not necessarily Internet) connectivity
between the parties. Given a BEET, arbitrary standard higher layer
protocols can then be used for Observer to Pilot (O2P)
communications (e.g., SIP [RFC3261] et seq), V2X communications
(e.g., [MAVLink]), etc. This approach satisfies DRIP requirement
GEN-6 Contact, supports satisfaction of requirements [I-D.ietf-drip-
reqs] GEN-8, GEN-9, PRIV-2, PRIV-5 and REG-3, and is compatible with
all other DRIP requirements.

9. IANA Considerations

This document does not make any IANA request.

10. 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.

11. Privacy & Transparency Considerations

Broadcast RID messages can contain Personally Identifiable Information (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. Authorized Observers could obtain plaintext in either of two ways. An Observer can send the UAS ID and the cyphertext to a server that offers decryption as a service. An Observer can send the UAS ID only to a server that returns the session key, so that 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 it can be, from the UAS ID itself). 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 MUST 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.

12. References

12.1. Normative References

[I-D.ietf-drip-reqs] Card, S. W., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-18, 8 September 2021, <https://www.ietf.org/archive/id/draft-ietf-drip-reqs-18.txt>.

[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>.

12.2. 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] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[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>.

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

[I-D.ietf-drip-auth] Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats & Protocols for Broadcast Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-auth-04, 20 December 2021, <https://www.ietf.org/archive/id/draft-ietf-drip-auth-04.txt>.

[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/>.

[MAVLink]
          "Micro Air Vehicle Communication Protocol", 2021,
          <http://mavlink.io/>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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 integration 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 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 UTM envisioned functionality. The LAANC program can automate the UAS operational intent (flight plan) submission and application for airspace authorization in real-time by checking against multiple aeronautical databases such as airspace classification and operating rules

associated with it, 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 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 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 (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 the 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.

Authors' Addresses

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

   Email: stu.card@axenterprize.com

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

   Email: adam.wiethuechter@axenterprize.com

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

   Email: rgm@labs.htt-consult.com

   Shuai Zhao
   Tencent
   2747 Park Blvd
   Palo Alto, 94588

United States of America

Email: shuai.zhao@ieee.org

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping Linköping
Sweden

Email: gurtov@acm.org