Project ICARUS

QL-Robotics

Intended status: CONFIDENTIAL

Expires: 14 May 2023

Drone Remote Identification Protocol (DRIP) Architecture

Laurens Martha (lead engineer)

Boris Huechter (engineer)

Danny Moskov (IETF)

Anton Goertov (IETF)

Mary Lim-Lee (legal)

Abstract

This document describes the architecture for protocols and services to support Unmanned Aircraft System Remote Identification and trackinget (UAS RID), plus RID-related communications.

Status of This Memo

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

This draft will expire on 14 May 2023.

Copyright Notice

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.

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.

Figure 1

Broadcast RID provides information only about unmanned aircraft (UA) within direct RF LOS, typically similar to visual Light-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

Using the same data dictionary that is the basis of Broadcast RID messages defines Network Remote Identification 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, e.g. their respective GNSS derived locations).
- 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 query for details on 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:

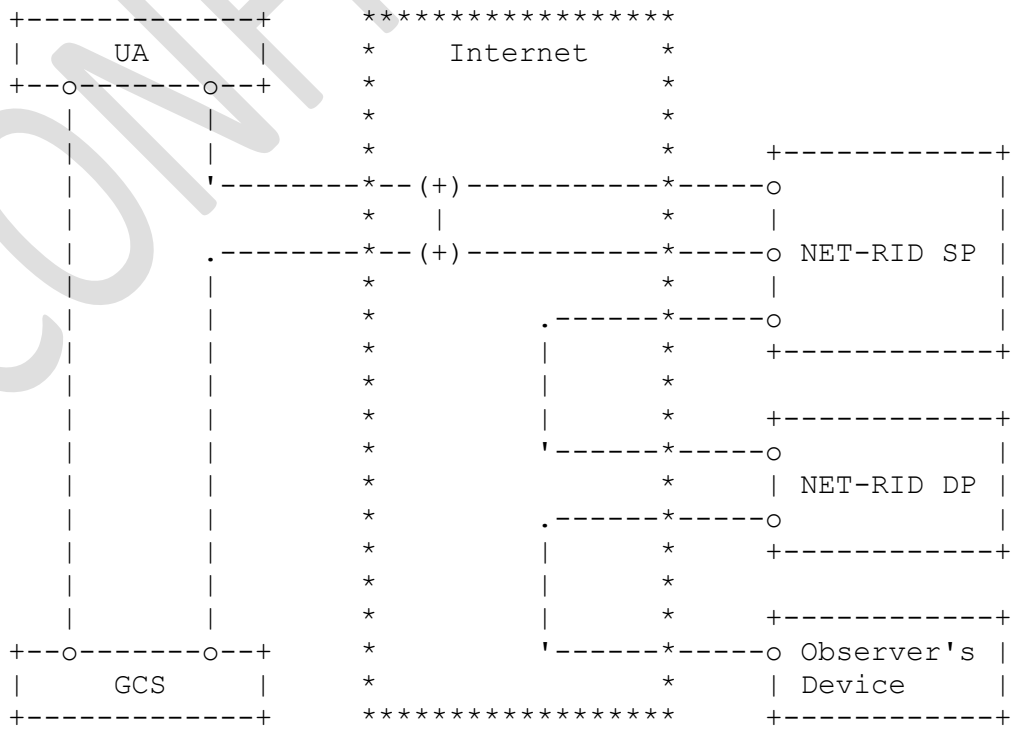

Figure 2

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.

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 Discovery and Synchronization Service (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 the UAS and its USS. With Broadcast-RID and UTM, 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 Surveillance Supplemental Data Service Provider (SDSP). 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.

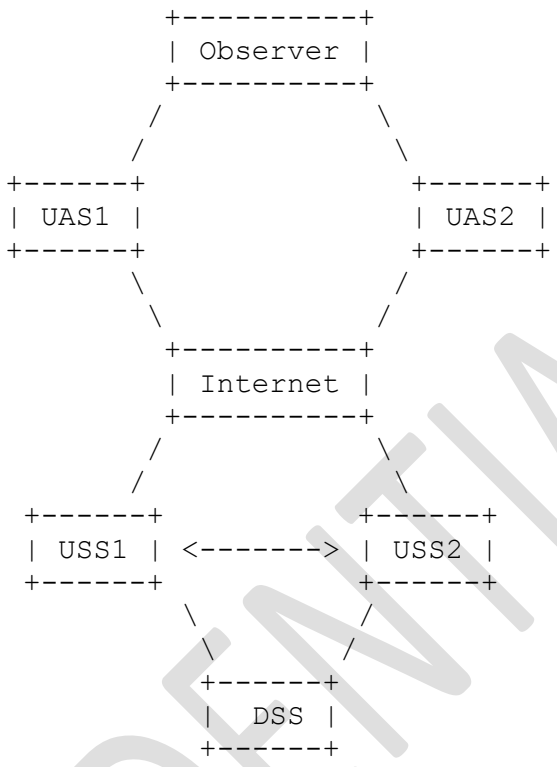

Figure 3

Editor-note-1: (Boris) re-draw this figure and propose text. Then double check the langauge in Editor-note-8

1.4. Overview of DRIP Architecture

Figure 4 illustrates a brief summary of the general UAS RID usage scenarios in DRIP.

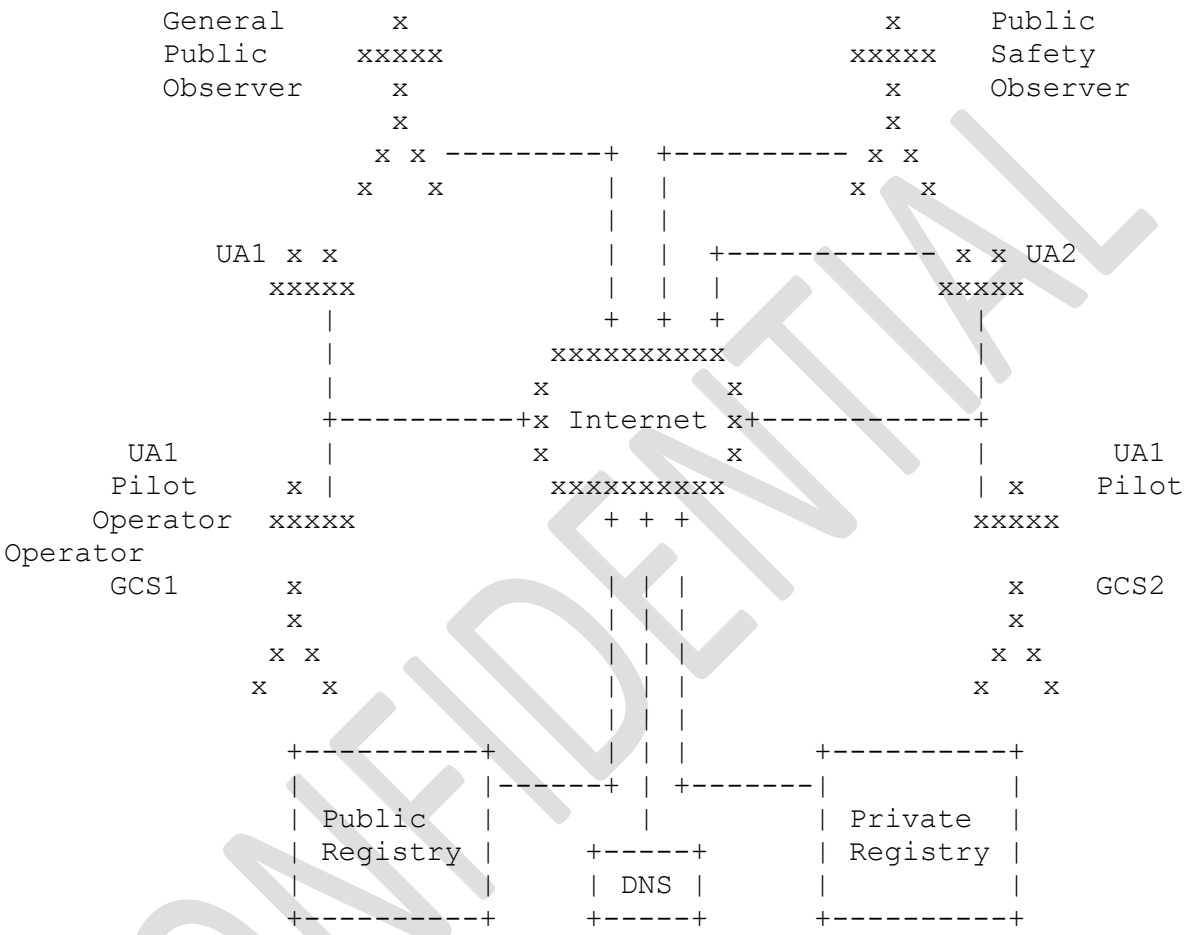

Figure 4

Editor-note-2: Laurens: place figure 4 on portfolio on website

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) ([RFC7482]) 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. Terms and Definitions

2.1. Architecture Terminology

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

2.2. Abbreviations

EdDSA: Edwards-Curve Digital Signature Algorithm

HHIT: Hierarchical HIT

HIP: Host Identity Protocol

HIT: Host Identity Tag

2.3. Additional Definitions

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

3. Claims, Assertions, Attestations, and Certificates

Editor-note-7: (Laurens) move section 3 to Section 2.4?

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) its signing over.

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 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: that the only way for any other entity to prove ownership of that identifier would be to obtain information that ought to be available only to the legitimate owner of the identifier (e.g., a cryptographic private key). 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, Session IDs, 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. 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 basic HIT 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.

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).

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, 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.

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.

Editor-note-3: review the last/above pragraph.

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 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. 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 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

Editor-note-4: Section 5 needs to cite the corresponding numbered requirement that it supports. 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.

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] [RFC7482] [RFC7483]). 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

Editor-note-5: Section 6 doesn't use the word "authentication" in the

section title, is there a reason to avoid it?

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). 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.

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) 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

Editor-note-6: Section 7 needs to cite the corresponding numbered requirement that it supports.

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.

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 including 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.

Editor-note-8: double check above paragraph after Editor-note-1 is resolved.

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. 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.

10. 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.