Drone Remote Identification Protocol (DRIP) Architecture
draft-ietf-drip-arch-23

Abstract

This document describes an architecture for protocols and services to
support Unmanned Aircraft System (UAS) Remote Identification (RID)
and tracking, plus UAS RID-related communications. This architecture
adheres to the requirements listed in the DRIP Requirements document
(RFC9153).

Status of This Memo

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

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

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

This Internet-Draft will expire on 2 December 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
license-info) in effect on the date of publication of this document.
Internet-Draft              DRIP Architecture                   May 2022

Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction .............................................. 3
   1.1. Overview of Unmanned Aircraft System (UAS) Remote ID (RID) and Standardization .................. 3
   1.2. Overview of Types of UAS Remote ID ................. 4
       1.2.1. Broadcast RID ................................... 4
       1.2.2. Network RID ...................................... 5
   1.3. Overview of USS Interoperability .................... 7
   1.4. Overview of DRIP Architecture ....................... 8
2. Terms and Definitions ..................................... 10
   2.1. Additional Abbreviations ............................. 10
   2.2. Additional Definitions ............................... 11
3. HHI as the DRIP Entity Identifier ........................ 11
   3.1. UAS Remote Identifiers Problem Space ............... 12
   3.2. HHI as A Trustworthy DRIP Entity Identifier ....... 12
   3.3. HHI for DRIP Identifier Registration and Lookup ... 14
   3.4. HHI as a Cryptographic Identifier .................. 14
4. DRIP Identifier Registration and Registries ............ 14
   4.1. Public Information Registry ........................ 15
       4.1.1. Background ...................................... 15
       4.1.2. DNS as the Public DRIP Identifier Registry .... 15
   4.2. Private Information Registry ....................... 15
       4.2.1. Background ...................................... 15
       4.2.2. EPP and RDAP as the Private DRIP Identifier Registry ........................................... 16
       4.2.3. Alternative Private DRIP Registry methods .... 16
5. DRIP Identifier Trust .................................... 16
6. Harvesting Broadcast Remote ID messages for UTM Inclusion 17
   6.1. The CS-RID Finder .................................... 18
   6.2. The CS-RID SDSP ..................................... 18
7. DRIP Contact ............................................ 18
8. Security Considerations .................................. 19
   8.1. Post Quantum Computing out of scope ................ 20
9. Privacy & Transparency Considerations .................... 20
10. References ............................................. 20
    10.1. Normative References .............................. 20
    10.2. Informative References ............................ 21
Appendix A. Overview of Unmanned Aircraft Systems (UAS) Traffic Management (UTM) ......................... 24
    A.1. Operation Concept ................................... 24
    A.2. UAS Service Supplier (USS) ........................ 25

1. Introduction

This document describes an architecture for protocols and services to support Unmanned Aircraft System (UAS) Remote Identification (RID) and tracking, 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 [RFC9153]. 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 that enables a UAS to be identified by Unmanned Aircraft Systems Traffic Management (UTM) and UAS Service Supplier (USS) (Appendix A) or third party 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.

USA Federal Aviation Administration (FAA)

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

European Union Aviation Safety Agency (EASA)

The EASA published a [Delegated] regulation in 2019 imposing requirements on UAS manufacturers and third-country operators, including but not limited to UAS RID requirements. The same year, EASA also published an [Implementing] regulation laying down
detailed rules and procedures for UAS operations and operating personnel then was updated in 2021 [Implementing_update]. A Notice of Proposed Amendment [NPA] was published in 2021 to provide more information about the development of acceptable means of compliance and guidance material to support the U-space regulation.

American Society for Testing and Materials (ASTM)


ASTM defines one set of UAS 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 the FAA in its UAS 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 services that can be offered based on UAS 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 UAS RID discussed in Section 3 may be used as the 3GPP CAA-level UAS ID for Remote Identification purposes.

1.2. Overview of Types of UAS Remote ID

This specification introduces two types UAS Remote ID defined in ASTM [F3411].

1.2.1. Broadcast RID

[F3411] defines a set of UAS 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) |
+------------------------+
    app messages directly over one-way RF data link (no IP)
    v
+------------------------+
| Observer's device (e.g., smartphone) |
+------------------------+
```

Figure 1

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

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 UAS RID is generated by the UAS. Typically some of this data is generated by the UA and some by the GCS (Ground Control Station), e.g., their respective Global Navigation Satellite System (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 (Section 2.2 of [RFC9153]), describing the volumes but not the operations.
* An Observer’s device, which is expected, 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:

![Diagram of Net-RID data flow](image)

Figure 2

Command and Control (C2) must flow from the GCS to the UA via some path. Currently (in the year 2022) this is typically a direct RF link; however, with increasing Beyond Visual Line of Sight (BVLOS) operations, it is expected often to be a wireless link 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, UAS RID information pertaining to both the GCS and the UA can be sent, by whichever has Internet connectivity, to the Net-RID SP, typically the USS managing the UAS operation.

The Net-RID SP forwards UAS RID information via the Internet to subscribed Net-RID DPs, typically USS. Subscribed Net-RID DPs then forward RID information via the Internet to subscribed Observer devices. Regulations require and [F3411] describes UAS 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 the Observer and the 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 UAS 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.
1.4. Overview of DRIP Architecture

Figure 4 illustrates a global UAS RID usage scenario. Broadcast RID links are not shown as they reach from any UA to any listening receiver in range and thus would obscure the intent of the figure. Figure 4 shows, as context, some entities and interfaces beyond the scope of DRIP (as currently (2022) chartered).
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:

Figure 4

DAA: Detect And Avoid
GPOD: General Public Observer Device
PSOD: Public Safety Observer Device
V2I: Vehicle-to-Infrastructure
V2V: Vehicle-to-Vehicle
- Design of trustworthy remote identifiers (Section 3).

- 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 4.1 and Section 4.2).

- Specific authentication methods and message payload formats to enable verification that Broadcast RID messages were sent by the claimed sender (Section 5) and that sender is in the claimed registry (Section 4 and Section 5).

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

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

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

2. Terms and Definitions

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

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

This document uses terms defined in [RFC9153].

2.1. Additional Abbreviations

DET: DRIP Entity Tag
EdDSA: Edwards-Curve Digital Signature Algorithm
HHIT: Hierarchical HIT
HI: Host Identity

2.2. Additional Definitions

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. 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) [RFC7401] as self-asserting IPv6 addresses suitable as a UAS ID type and, more generally, as trustworthy multipurpose remote identifiers.
Self-asserting in this usage means that, given the Host Identity (HI), the HHIT ORCHID construction and a signature of the registry on the HHIT, the HHIT can be verified by the receiver. The explicit registration hierarchy within the HHIT provides registry discovery (managed by a Registrar) to either yield the HI for a 3rd-party (seeking UAS ID attestation) validation or prove that the HHIT and HI have been registered uniquely.

3.1. UAS Remote Identifiers Problem Space

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

Broadcast RID, especially its support for Bluetooth 4, imposes severe constraints. ASTM UAS 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 standards development organizations (SDOs) as extensions to ASTM UAS 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 UAS RID [F3411] Authentication Message payload is 201 bytes for most authentication types. A type 5 is also added in this revision for IETF and other SDOs to develop Specific Authentication Methods as extensions to ASTM UAS RID. One byte out of 201 bytes is consumed to index the sub-type which leaves only 200 for DRIP authentication payloads, including one or more DRIP entity identifiers and associated authentication data.

3.2. HHIT as A Trustworthy DRIP Entity Identifier

A Remote UAS ID that can be trustworthy for use in Broadcast RID can be built from an asymmetric keypair. In this method, the UAS ID is cryptographically derived directly from the public key. The proof of UAS ID ownership (verifiable attestation, versus mere claim) is guaranteed by signing this cryptographic UAS ID with the associated private key. The association between the UAS ID and the private key is ensured by cryptographically binding the public key with the UAS ID; more specifically, the UAS ID results from the hash of the public key. The public key is designated as the HI while the UAS ID is designated as the HIT.
By construction, the HIT is statistically unique through the 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 MUST be provisioned not only with its HHIT but also with the HI public key from which the HHIT was derived and the corresponding private key, to enable message signature. A UAS equipped for 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. Operators and Private Information Registries, as well as other UTM entities, can use HHITs for their IDs. Such HHITs can facilitate DRIP security functions such as 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 8).

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.
3.3. HHIT for DRIP Identifier Registration and Lookup

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

A DRIP registration process based on the explicit hierarchy within a HHIT provides manageable uniqueness of the HI for the HHIT. 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-served registration for a HHIT provides deterministic access to any other needed actionable information based on inquiry access authority (more details in Section 4.2).

3.4. HHIT as a Cryptographic Identifier

The only (known to the authors at the time of this writing) existing types of IP address compatible identifiers cryptographically derived from the public keys of the identified entities are Cryptographically Generated Addresses (CGAs) [RFC3972] and Host Identity Tags (HITs) [RFC7401]. CGAs and HITs lack registration/retrieval capability. To provide this, each HHIT embeds plaintext information designating the hierarchy within which it is registered 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.

4. DRIP Identifier Registration and Registries

DRIP registries hold both public and private UAS information (See PRIV-1 in [RFC9153]) resulting from the DRIP identifier registration process. Given these different uses, and to improve scalability, security, and simplicity of administration, the public and private information can be stored in different registries. This section introduces the public and private information registries for DRIP identifiers. This DRIP Identifier registration process satisfies the following DRIP requirements defined in [RFC9153]: GEN-3, GEN-4, ID-2, ID-4, ID-6, PRIV-3, PRIV-4, REG-1, REG-2, REG-3 and REG-4.
4.1. Public Information Registry

4.1.1. Background

The public information registry provides trustable information such as attestations of UAS 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 UAS 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 directly provide all public information registry information. The Net-RID DP is the only source of information for a query on an airspace volume.

4.1.2. 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).

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

4.2. Private Information Registry

4.2.1. Background

The private information required for DRIP identifiers is similar to that required for Internet domain name registration. A DRIP identifier solution can leverage existing Internet resources: registration protocols, infrastructure, and business models, by fitting into an UAS ID structure compatible with DNS names. The HHIT hierarchy can provide the needed scalability and management structure. It is expected that the private information registry function will be provided by the same organizations that run a USS, and likely integrated with a USS. The lookup function may be implemented by the Net-RID DPs.
4.2.2. 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].

4.2.3. 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.

5. DRIP Identifier Trust

While the DRIP entity identifier is self-asserting, it alone does not provide the trustworthiness (non-repudiability, protection vs. spoofing, message integrity protection, scalability, etc.) essential to UAS RID, as justified in [RFC9153]. For that it MUST be registered (under DRIP Registries) and be actively used by the party (in most cases the UA). A sender’s identity can not be approved by only possessing a DRIP Entity Tag (DET), 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, it 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.

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 UA’s claims.

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

6. Harvesting Broadcast Remote ID messages for UTM Inclusion

ASTM anticipated that regulators would require both Broadcast RID and Network RID for large UAS, but allow UAS RID requirements for small UAS to be satisfied with the operator’s choice of either Broadcast RID or Network RID. The EASA initially specified Broadcast RID for essentially all UAS, and is now also considering Network RID. The FAA UAS RID Final Rules [FAA_RID] permit only Broadcast RID for rule compliance, but still encourage Network RID for complementary functionality, especially in support of UTM.

One opportunity is to enhance the architecture with gateways from Broadcast RID to Network RID. This provides the best of both and gives regulators and operators flexibility. It offers advantages over either form of UAS RID alone: 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.

Multilateration technologies use physical layer information, such as precise Time Of Arrival (TOA) of transmissions from mobile transmitters at receivers with a priori precisely known locations, to estimate the locations of the mobile transmitters.
Further, gateways with additional sensors (e.g., smartphones with cameras) can provide independent information on the UA type and size, confirming or refuting those claims made in the UAS RID messages.

Section 6.1 and Section 6.2 define two additional entities that are required to provide this Crowd Sourced Remote ID (CS-RID).

This approach satisfies the following DRIP requirements defined in [RFC9153]: GEN-5, GEN-11, and REG-1.

6.1. The CS-RID Finder

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

6.2. 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.

7. 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 3 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 5 enable Observer verification of that relationship. A DRIP entity identifier with suitable records in public and private registries as outlined in Section 5 can enable lookup not only of information regarding the UAS, but also identities...
of and pointers to information regarding the various associated entities (e.g., the USS under which the UAS is flying an operation), including means of contacting those associated entities (i.e., locators, typically IP addresses).

A suitably equipped Observer could initiate a cryptographic handshake to a similarly 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; the USS, etc. Assuming mutual authentication is successful, keys can then be negotiated for an IPsec Encapsulating Security Payload (ESP) tunnel, over which 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. Certain preconditions are necessary: each party 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. One method directly supported by the use of HHITs as DRIP entity identifiers is initiation of a HIP Base Exchange (BEX) and Bound End-to-End Tunnel (BEET).

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

8. Security Considerations

The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. It may be necessary for the GCS to have the key pair to register the HHIT to the USS. Thus it may be the GCS that generates the key pair and delivers it to the UA, making the GCS a part of the key security boundary. Leakage of the private key either from the UA or GCS to the component manufacturer is a valid concern and steps need to be in place to ensure safe keeping of the private key.

The size of the public key hash in the HHIT is also of concern. It is well within current server array technology to compute another key pair that hashes to the same HHIT. Thus an adversary could impersonate a validly registered UA. This attack would only be exposed when the HI in DRIP authentication message is checked back to the USS and found not to match.
Finally, the UAS 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.

8.1. Post Quantum Computing out of scope

There has been no effort, at this time, to address post quantum computing cryptography. UAs and Broadcast Remote ID communications are so constrained that current post quantum computing cryptography is not applicable. Plus since a UA may use a unique HHIT for each operation, the attack window could be limited to the duration of the operation.

Finally, as the HHIT contains the ID for the cryptographic suite used in its creation, a future post quantum computing safe algorithm that fits the Remote ID constraints may readily be added.

9. 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.

10. References

10.1. Normative References

10.2. Informative References


Card, et al.
[I-D.ietf-drip-auth]

[Implementing]

[Implementing_update]


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 to integrate UAS operations into the national airspace system (NAS) led to the development of the concept of UTM and the ecosystem around it. The UTM concept was initially presented in 2013 and version 2.0 was published in 2020 [FAA_UAS_Concept_Of_Ops].
The eventual concept refinement, initial prototype implementation, and testing were conducted by the joint FAA and NASA UTM research transition team. World efforts took place afterward. The Single European Sky ATM Research (SESAR) started the CORUS project to research its UTM counterpart concept, namely [U-Space]. This effort is led by the European Organization for the Safety of Air Navigation (Eurocontrol).

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

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

A.2. UAS Service Supplier (USS)

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

The FAA works with UAS industry shareholders and promotes the Low Altitude Authorization and Notification Capability [LAANC] program, which is the first system to realize some of the envisioned functionality of UTM. The LAANC program can automate UAS operational intent (flight plan) 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 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 (e.g., 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 UAS. 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. Thanks to Alexandre Petrescu and Stephan Wenger for the helpful and positive comments. Thanks to chairs Daniel Migault and Mohamed Boucadair for direction of our team of authors and editor, some of whom are newcomers to writing IETF documents. Laura Welch is also thanked for her valuable review comments that led to great improvements of this memo. Thanks especially to Internet Area Director Eric Vyncke for guidance and support.

Authors’ Addresses

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY, 13495
United States of America
Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY, 13495
United States of America
Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI, 48237
United States of America
Email: rgm@labs.htt-consult.com

Shuai Zhao
Tencent
2747 Park Blvd
Palo Alto, 94306
United States of America
Email: shuai.zhao@ieee.org
Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping Linköping
Sweden
Email: gurtov@acm.org
This document defines terminology and requirements for Drone Remote Identification Protocol (DRIP) Working Group solutions to support Unmanned Aircraft System Remote Identification and tracking (UAS RID) for security, safety, and other purposes (e.g., initiation of identity based network sessions supporting UAS applications). DRIP will facilitate use of existing Internet resources to support RID and to enable enhanced related services, and will enable online and offline verification that RID information is trustworthy.
1. Introduction

For any unfamiliar or _a priori_ ambiguous terminology herein, see Section 2.

1.1. Motivation and External Influences

Many considerations (especially safety and security) necessitate Unmanned Aircraft Systems (UAS) Remote Identification and tracking (RID).

Unmanned Aircraft (UA) may be fixed wing, rotary wing (e.g., helicopter), hybrid, balloon, rocket, etc. Small fixed wing UA typically have Short Take-Off and Landing (STOL) capability; rotary wing and hybrid UA typically have Vertical Take-Off and Landing (VTOL) capability. UA may be single- or multi-engine. The most common today are multicopters: rotary wing, multi engine. The explosion in UAS was enabled by hobbyist development, for multicopters, of advanced flight stability algorithms, enabling even inexperienced pilots to take off, fly to a location of interest, hover, and return to the take-off location or land at a distance. UAS can be remotely piloted by a human (e.g., with a joystick) or programmed to proceed from Global Navigation Satellite System (GNSS) waypoint to waypoint in a weak form of autonomy; stronger autonomy is coming.

Small UA are "low observable" as they:

* typically have small radar cross sections;

* make noise quite noticeable at short ranges but difficult to detect at distances they can quickly close (500 meters in under 13 seconds by the fastest consumer mass market drones available in early 2021);

* typically fly at low altitudes (e.g., for those to which RID applies in the US, under 400 feet Above Ground Level (AGL) as per [Part107]);

* are highly maneuverable so can fly under trees and between buildings.

UA can carry payloads including sensors, cyber and kinetic weapons, or can be used themselves as weapons by flying them into targets. They can be flown by clueless, careless, or criminal operators. Thus the most basic function of UAS RID is "Identification Friend or Foe" (IFF) to mitigate the significant threat they present.
Diverse other applications can be enabled or facilitated by RID. Internet protocols typically start out with at least one entity already knowing an identifier or locator of another; but an entity (e.g., UAS or Observer device) encountering an _a priori_ unknown UA in physical space has no identifier or logical space locator for that UA, unless and until one is provided somehow. RID provides an identifier, which, if well chosen, can facilitate use of a variety of Internet family protocols and services to support arbitrary applications, beyond the basic security functions of RID. For most of these, some type of identifier is essential, e.g., Network Access Identifier (NAI), Digital Object Identifier (DOI), Uniform Resource Identifier (URI), domain name, or public key. DRIP motivations include both the basic security and the broader application support functions of RID. The general scenario is illustrated in Figure 1.

![Diagram of UAS RID Usage Scenario](image)

Figure 1: "General UAS RID Usage Scenario"

Figure 1 illustrates a typical case where there may be: multiple Observers, some of them members of the general public, others government officers with public safety/security responsibilities; multiple UA in flight within observation range, each with its own pilot/operator; at least one registry each for lookup of public and
(by authorized parties only) private information regarding the UAS and their pilots/operators; and in the DRIP vision, DNS resolving various identifiers and locators of the entities involved.

Note the absence of any links to/from the UA in the figure; this is because UAS RID and other connectivity involving the UA varies. Some connectivity paths do or do not exist depending upon the scenario. Command and Control (C2) from the GCS to the UA via the Internet (e.g., using LTE cellular) is expected to become much more common as Beyond Visual Line Of Sight (BVLOS) operations increase; in such a case, there is typically not also a direct wireless link between the GCS and UA. Conversely, if C2 is running over a direct wireless link, then typically the GCS has but the UA lacks Internet connectivity. Further, paths that nominally exist, such as between an Observer device and the Internet, may be severely intermittent. These connectivity constraints are likely to have an impact, e.g., on how reliably DRIP requirements can be satisfied.

An Observer of UA may need to classify them, as illustrated notionally in Figure 2, for basic airspace Situational Awareness (SA). An Observer who classifies a UAS: as Taskable, can ask it to do something useful; as Low Concern, can reasonably assume it is not malicious and would cooperate with requests to modify its flight plans for safety concerns that arise; as High Concern or Unidentified, can focus surveillance on it.

| +--------------+ +--------------+ +--------------+ |
|  Taskable     |  Low Concern  |  High Concern |
| +--------------+ +--------------+ +--------------+ |

Figure 2: "Notional UAS Classification"
ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed the widely cited Standard Specification for Remote ID and Tracking [F3411-19]: the published standard is available for purchase from ASTM and as an ASTM membership premium; early drafts are freely available as [OpenDroneID] specifications. [F3411-19] is frequently referenced in DRIP, where building upon its link layers and both enhancing support for and expanding the scope of its applications are central foci.

In many applications, including UAS RID, identification and identifiers are not ends in themselves; they exist to enable lookups and provision of other services.

Using UAS RID to facilitate vehicular (V2X) communications and applications such as Detect And Avoid (DAA), which would impose tighter latency bounds than RID itself, is an obvious possibility, explicitly contemplated in the United States (US) Federal Aviation Administration (FAA) Remote Identification of Unmanned Aircraft rule [FRUR]. However, usage of RID systems and information beyond mere identification (primarily to hold operators accountable after the fact), including DAA, have been declared out of scope in ASTM F38.02 WK65041, based on a distinction between RID as a security standard vs DAA as a safety application. Aviation community Standards Development Organizations (SDOs) generally set a higher bar for safety than for security, especially with respect to reliability. Each SDO has its own cultural set of connotations of safety vs security; the denotative definitions of the International Civil Aviation Organization (ICAO) are cited in Section 2.

[Opinion1] and [WG105] cite the Direct Remote Identification (DRI) previously required and specified, explicitly stating that whereas DRI is primarily for security purposes, the "Network Identification Service" [Opinion1] (in the context of U-space [InitialView]) or "Electronic Identification" [WG105] is primarily for safety purposes (e.g., Air Traffic Management, especially hazards deconfliction) and also is allowed to be used for other purposes such as support of efficient operations. These emerging standards allow the security and safety oriented systems to be separate or merged. In addition to mandating both Broadcast and Network one-way to Observers, they will use V2V to other UAS (also likely to and/or from some manned aircraft). These reflect the broad scope of the European Union (EU) U-space concept, as being developed in the Single European Sky ATM Research (SESAR) Joint Undertaking, the U-space architectural principles of which are outlined in [InitialView].

ASD-STAN is an Associated Body to CEN (European Committee for Standardization) for Aerospace Standards. It is publishing an EU standard "Aerospace series - Unmanned Aircraft Systems - Part 002:
Direct Remote Identification; English version prEN 4709-002:2020" for which a current (early 2021) informal overview is freely available in [ASDRI]. It will provide compliance to cover the identical DRI requirements applicable to drones of classes C1 - [Delegated] Part 2, C2 - [Delegated] Part 3, C3 - [Delegated] Part 4, C5 - [Amended] Part 16, and C6 - [Amended] Part 17.

The standard contemplated in [ASDRI] will provide UA capability to be identified in real time during the whole duration of the flight, without specific connectivity or ground infrastructure link, utilizing existing mobile devices within broadcast range. It will use Bluetooth 4, Bluetooth 5, Wi-Fi Neighbor Awareness Networking (NAN, also known as Wi-Fi Aware, [WiFiNAN]) and/or IEEE 802.11 Beacon modes. The EU standard emphasis was compatibility with [F3411-19], although there are differences in mandatory and optional message types and fields.

The [ASDRI] contemplated DRI system will broadcast locally:

1. the UAS operator registration number;
2. the [CTA2063A] compliant unique serial number of the UA;
3. a time stamp, the geographical position of the UA, and its height AGL or above its take-off point;
4. the UA ground speed and route course measured clockwise from true north;
5. the geographical position of the remote pilot, or if that is not available, the geographical position of the UA take-off point; and
6. for Classes C1, C2, C3, the UAS emergency status.

Under the [ASDRI] contemplated standard, data will be sent in plain text and the UAS operator registration number will be represented as a 16-byte string including the (European) state code. The corresponding private ID part will contain 3 characters that are not broadcast but used by authorities to access regional registration databases for verification.

ASD-STAN also contemplates corresponding Network Remote Identification (NRI) functionality. The ASD-STAN RID target is to revise their current standard with additional functionality (e.g., DRIP) to be published before 2022 [ASDRI].
Security oriented UAS RID essentially has two goals: enable the general public to obtain and record an opaque ID for any observed UA, which they can then report to authorities; and enable authorities, from such an ID, to look up information about the UAS and its operator. Safety oriented UAS RID has stronger requirements.

Although dynamic establishment of secure communications between the Observer and the UAS pilot seems to have been contemplated by the FAA UAS ID and Tracking Aviation Rulemaking Committee (ARC) in their [Recommendations], it is not addressed in any of the subsequent regulations or international SDO technical specifications, other than DRIP, known to the authors as of early 2021.

1.2. Concerns and Constraints

Disambiguation of multiple UA flying in close proximity may be very challenging, even if each is reporting its identity, position, and velocity as accurately as it can.

The origin of information in UAS RID and UAS Traffic Management (UTM) generally is the UAS or its operator. Self-reports may be initiated by the remote pilot at the console of the Ground Control Station (GCS, the UAS subsystem used to remotely operate the UA), or automatically by GCS software; in Broadcast RID, they typically would be initiated automatically by a process on the UA. Data in the reports may come from sensors available to the operator (e.g., radar or cameras), the GCS (e.g., "dead reckoning" UA location, starting from the takeoff location and estimating the displacements due to subsequent piloting commands, wind, etc.), or the UA itself (e.g., an on-board GNSS receiver); in Broadcast RID, all the data must be sent proximately by, and most of the data comes ultimately from, the UA itself. Whether information comes proximately from the operator, or from automated systems configured by the operator, there are possibilities not only of unintentional error in but also of intentional falsification of this data. Mandating UAS RID, specifying data elements required to be sent, monitoring compliance and enforcing it (or penalizing non-compliance) are matters for Civil Aviation Authorities (CAAs) et al; specifying message formats, etc. to carry those data elements has been addressed by other SDOs; offering technical means, as extensions to external standards, to facilitate verifiable compliance and enforcement/monitoring, are opportunities for DRIP.

Minimal specified information must be made available to the public. Access to other data, e.g., UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized in accordance with applicable policy. The balance between privacy and transparency remains a subject for
public debate and regulatory action; DRIP can only offer tools to expand the achievable trade space and enable trade-offs within that space. [F3411-19], the basis for most current (2021) thinking about and efforts to provide UAS RID, specifies only how to get the UAS ID to the Observer: how the Observer can perform these lookups and how the registries first can be populated with information are unspecified therein.

The need for nearly universal deployment of UAS RID is pressing: consider how negligible the value of an automobile license plate system would be if only 90% of the cars displayed plates. This implies the need to support use by Observers of already ubiquitous mobile devices (typically smartphones and tablets). Anticipating CAA requirements to support legacy devices, especially in light of [Recommendations], [F3411-19] specifies that any UAS sending Broadcast RID over Bluetooth must do so over Bluetooth 4, regardless of whether it also does so over newer versions; as UAS sender devices and Observer receiver devices are unpaired, this implies extremely short "advertisement" (beacon) frames.

Wireless data links to or from UA are challenging. Flight is often amidst structures and foliage at low altitudes over varied terrain. UA are constrained in both total energy and instantaneous power by their batteries. Small UA imply small antennas. Densely populated volumes will suffer from link congestion: even if UA in an airspace volume are few, other transmitters nearby on the ground, sharing the same license free spectral band, may be many. Thus air to air and air to ground links will generally be slow and unreliable.

UAS Cost, Size, Weight, and Power (CSWaP) constraints are severe. CSWaP is a burden not only on the designers of new UAS for sale, but also on owners of existing UAS that must be retrofit. Radio Controlled (RC) aircraft modelers, "hams" who use licensed amateur radio frequencies to control UAS, drone hobbyists, and others who custom build UAS, all need means of participating in UAS RID, sensitive to both generic CSWaP and application-specific considerations.

To accommodate the most severely constrained cases, all these conspire to motivate system design decisions that complicate the protocol design problem.

Broadcast RID uses one-way local data links. UAS may have Internet connectivity only intermittently, or not at all, during flight.

Internet-disconnected operation of Observer devices has been deemed by ASTM F38.02 too infrequent to address. However, the preamble to [FRUR] cites "remote and rural areas that do not have reliable
Internet access" as a major reason for requiring Broadcast rather than Network RID, and states that "Personal wireless devices that are capable of receiving 47 CFR part 15 frequencies, such as smart phones, tablets, or other similar commercially available devices, will be able to receive broadcast remote identification information directly without reliance on an Internet connection". Internet-disconnected operation presents challenges, e.g., for Observers needing access to the [F3411-19] web based Broadcast Authentication Verifier Service or needing to do external lookups.

As RID must often operate within these constraints, heavyweight cryptographic security protocols or even simple cryptographic handshakes are infeasible, yet trustworthiness of UAS RID information is essential. Under [F3411-19], _even the most basic datum, the UAS ID itself, can be merely an unsubstantiated claim_.

Observer devices being ubiquitous, thus popular targets for malware or other compromise, cannot be generally trusted (although the user of each device is compelled to trust that device, to some extent); a "fair witness" functionality (inspired by [Stranger]) is desirable.

Despite work by regulators and SDOs, there are substantial gaps in UAS standards generally and UAS RID specifically. [Roadmap] catalogs UAS related standards, ongoing standardization activities and gaps (as of 2020); Section 7.8 catalogs those related specifically to UAS RID. DRIP will address the most fundamental of these gaps, as foreshadowed above.

1.3. DRIP Scope

DRIP’s initial charter is to make RID immediately actionable, in both Internet and local-only connected scenarios (especially emergencies), in severely constrained UAS environments, balancing legitimate (e.g., public safety) authorities’ Need To Know trustworthy information with UAS operators’ privacy. By "immediately actionable" is meant information of sufficient precision, accuracy, timeliness, etc. for an Observer to use it as the basis for immediate decisive action, whether that be to trigger a defensive counter-UAS system, to attempt to initiate communications with the UAS operator, to accept the presence of the UAS in the airspace where/when observed as not requiring further action, or whatever, with potentially severe consequences of any action or inaction chosen based on that information. For further explanation of the concept of immediate actionability, see [ENISACSIERT].

Note that UAS RID must achieve nearly universal adoption, but DRIP can add value even if only selectively deployed. Authorities with jurisdiction over more sensitive airspace volumes may set a higher
than generally mandated RID requirement for flight in such volumes. Those with a greater need for high-confidence IFF can equip with DRIP, enabling strong authentication of their own aircraft and allied operators without regard for the weaker (if any) authentication of others.

DRIP (originally Trustworthy Multipurpose Remote Identification, TM-RID) potentially could be applied to verifiably identify other types of registered things reported to be in specified physical locations, and providing timely trustworthy identification data is also prerequisite to identity-oriented networking, but the urgent motivation and clear initial focus is UAS. Existing Internet resources (protocol standards, services, infrastructure, and business models) should be leveraged.

1.4. Document Scope

This document describes the problem space for UAS RID conforming to proposed regulations and external technical standards, defines common terminology, specifies numbered requirements for DRIP, identifies some important considerations (IANA, security, privacy and transparency), and discusses limitations.

A natural Internet-based approach to meet these requirements is described in a companion architecture document [drip-architecture] and elaborated in other DRIP documents.

2. Terms and Definitions

2.1. Requirements Terminology

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

2.2. Definitions

This section defines a non-comprehensive set of terms expected to be used in DRIP documents. This list is meant to be the DRIP terminology reference; as such, some of the terms listed below are not used in this document.

[RFC4949] provides a glossary of Internet security terms that should be used where applicable.
In the UAS community, the plural form of acronyms generally is the same as the singular form, e.g., Unmanned Aircraft System (singular) and Unmanned Aircraft Systems (plural) are both represented as UAS. On this and other terminological issues, to encourage comprehension necessary for adoption of DRIP by the intended user community, that community’s norms are respected herein, and definitions are quoted in cases where they have been found in that community’s documents. Most of the listed terms are from that community (even if specific source documents are not cited); any that are DRIP-specific or invented by the authors of this document are marked "(DRIP)".

4-D
Four-dimensional. Latitude, Longitude, Altitude, Time. Used especially to delineate an airspace volume in which an operation is being or will be conducted.

AAA
Attestation, Authentication, Authorization, Access Control, Accounting, Attribution, Audit, or any subset thereof (uses differ by application, author, and context). (DRIP)

ABDAA
AirBorne DAA. Accomplished using systems onboard the aircraft involved. Supports "self-separation" (remaining "well clear" of other aircraft) and collision avoidance.

ADS-B
Automatic Dependent Surveillance – Broadcast. "ADS-B Out" equipment obtains aircraft position from other on-board systems (typically GNSS) and periodically broadcasts it to "ADS-B In" equipped entities, including other aircraft, ground stations, and satellite based monitoring systems.

AGL
Above Ground Level. Relative altitude, above the variously defined local ground level, typically of a UA, measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (GNSS) altitude.

ATC
Air Traffic Control. Explicit flight direction to pilots from ground controllers. Contrast with ATM.

ATM
Air Traffic Management. A broader functional and geographic scope and/or a higher layer of abstraction than ATC. "The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow
management - safely, economically and efficiently - through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions" [ICAOATM].

Authentication Message
[F3411-19] Message Type 2. Provides framing for authentication data, only; the only message that can be extended in length by segmenting it across more than one page.

Basic ID Message
[F3411-19] Message Type 0. Provides UA Type, UAS ID Type (and Specific Session ID subtype if applicable), and UAS ID, only.

Broadcast Authentication Verifier Service
System component designed to handle any authentication of Broadcast RID by offloading signature verification to a web service [F3411-19].

BVLOS
Beyond Visual Line Of Sight. See VLOS.

byte
Used here in its now-customary sense as a synonym for "octet", as "byte" is used exclusively in definitions of data structures specified in [F3411-19]

CAA
Civil Aviation Authority of a regulatory jurisdiction. Often so named, but other examples include the United States Federal Aviation Administration (FAA) and the Japan Civil Aviation Bureau.

CSWaP
Cost, Size, Weight, and Power.

C2
Command and Control. Previously mostly used in military contexts. Properly refers to a function, exercisable over arbitrary communications; but in the small UAS context, often refers to the communications (typically RF data link) over which the GCS controls the UA.

DAA
Detect And Avoid, formerly Sense And Avoid (SAA). A means of keeping aircraft "well clear" of each other and obstacles for safety. "The capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action to comply with the applicable rules of flight" [ICAOUAS].
DRI (not to be confused with DRIP)
Direct Remote Identification. EU regulatory requirement for "a system that ensures the local broadcast of information about a UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA". [Delegated] that presumably can be satisfied with appropriately configured [F3411-19] Broadcast RID.

DSS
Discovery and Synchronization Service. The UTM system overlay network backbone. Most importantly, it enables one USS to learn which other USS have UAS operating in a given 4-D airspace volume, for strategic deconfliction of planned operations and Network RID surveillance of active operations. [F3411-19]

EUROCAE
European Organisation for Civil Aviation Equipment. Aviation SDO, originally European, now with broader membership. Cooperates extensively with RTCA.

GBDAA
Ground Based DAA. Accomplished with the aid of ground based functions.

GCS
Ground Control Station. The part of the UAS that the remote pilot uses to exercise C2 over the UA, whether by remotely exercising UA flight controls to fly the UA, by setting GNSS waypoints, or otherwise directing its flight.

GNSS
Global Navigation Satellite System. Satellite based timing and/or positioning with global coverage, often used to support navigation.

GPS
Global Positioning System. A specific GNSS, but in the UAS context, the term is typically misused in place of the more generic term GNSS.

GRAIN
Global Resilient Aviation Interoperable Network. ICAO managed IPv6 overlay internetwork based on IATF, dedicated to aviation (but not just aircraft). Currently (2021) in design, accommodating the proposed DRIP identifier.
IATF
International Aviation Trust Framework. ICAO effort to develop a resilient and secure by design framework for networking in support of all aspects of aviation.

ICAO
International Civil Aviation Organization. A United Nations specialized agency that develops and harmonizes international standards relating to aviation.

IFF
Identification Friend or Foe. Originally, and in its narrow sense still, a self-identification broadcast in response to interrogation via radar, to reduce friendly fire incidents, which led to military and commercial transponder systems such as ADS-B. In the broader sense used here, any process intended to distinguish friendly from potentially hostile UA or other entities encountered.

LAANC
Low Altitude Authorization and Notification Capability. Supports ATC authorization requirements for UAS operations: remote pilots can apply to receive a near real-time authorization for operations under 400 feet in controlled airspace near airports. FAA authorized partial stopgap in the US until UTM comes.

Location/Vector Message
[F3411-19] Message Type 1. Provides UA location, altitude, heading, speed, and status.

LOS
Line Of Sight. An adjectival phrase describing any information transfer that travels in a nearly straight line (e.g., electromagnetic energy, whether in the visual light, RF, or other frequency range) and is subject to blockage. A term to be avoided due to ambiguity, in this context, between RF LOS and VLOS.

Message Pack
[F3411-19] Message Type 15. The framed concatenation, in message type index order, of at most one message of each type of any subset of the other types. Required to be sent in Wi-Fi NAN and in Bluetooth 5 Extended Advertisements, if those media are used; cannot be sent in Bluetooth 4.
MSL
Mean Sea Level. Shorthand for relative altitude, above the variously defined mean sea level, typically of a UA (but in [FRUR] also for a GCS), measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (e.g., as indicated by GNSS, referenced to the WGS84 ellipsoid).

Net-RID DP
Network RID Display Provider. [F3411-19] logical entity that aggregates data from Net-RID SPs as needed in response to user queries regarding UAS operating within specified airspace volumes, to enable display by a user application on a user device. Potentially could provide not only information sent via UAS RID but also information retrieved from UAS RID registries or information beyond UAS RID. Under superseded [NPRM], not recognized as a distinct entity, but a service provided by USS, including Public Safety USS that may exist primarily for this purpose rather than to manage any subscribed UAS.

Net-RID SP
Network RID Service Provider. [F3411-19] logical entity that collects RID messages from UAS and responds to NetRID-DP queries for information on UAS of which it is aware. Under superseded [NPRM], the USS to which the UAS is subscribed ("Remote ID USS").

Network Identification Service
EU regulatory requirement in [Opinion1] and [WG105] that presumably can be satisfied with appropriately configured [F3411-19] Network RID.

Observer
An entity (typically but not necessarily an individual human) who has directly or indirectly observed a UA and wishes to know something about it, starting with its ID. An Observer typically is on the ground and local (within VLOS of an observed UA), but could be remote (observing via Network RID or other surveillance), operating another UA, aboard another aircraft, etc. (DRIP)

Operation
A flight, or series of flights of the same mission, by the same UAS, separated by at most brief ground intervals. (Inferred from UTM usage, no formal definition found)

Operator
"A person, organization or enterprise engaged in or offering to engage in an aircraft operation" [ICAOUAS].
Operator ID Message
[F3411-19] Message Type 5. Provides CAA issued Operator ID, only. Operator ID is distinct from UAS ID.

Payload of a frame, containing a chunk of a message that has been segmented, to allow transport of a message longer than can be encapsulated in a single frame. [F3411-19]

PIC
Pilot In Command. "The pilot designated by the operator, or in the case of general aviation, the owner, as being in command and charged with the safe conduct of a flight" [ICAOUAS].

PII
Personally Identifiable Information. In the UAS RID context, typically of the UAS Operator, Pilot In Command (PIC), or Remote Pilot, but possibly of an Observer or other party. This specific term is used primarily in the US; other terms with essentially the same meaning are more common in other jurisdictions (e.g., "personal data" in the EU). Used herein generically to refer to personal information, which the person might wish to keep private, or may have a statutorily recognized right to keep private (e.g., under the EU [GDPR]), potentially imposing (legally or ethically) a confidentiality requirement on protocols/systems.

Remote Pilot
A pilot using a GCS to exercise proximate control of a UA. Either the PIC or under the supervision of the PIC. "The person who manipulates the flight controls of a remotely-piloted aircraft during flight time" [ICAOUAS].

RF
Radio Frequency. Adjective, e.g., "RF link", or noun.

RF LOS
RF Line Of Sight. Typically used in describing a direct radio link between a GCS and the UA under its control, potentially subject to blockage by foliage, structures, terrain, or other vehicles, but less so than VLOS.

RTCA
Radio Technical Commission for Aeronautics. US aviation SDO. Cooperates extensively with EUROCAE.
Safety
"The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level." From Annex 19 of the Chicago Convention, quoted in [ICAODEFS]

Security
"Safeguarding civil aviation against acts of unlawful interference." From Annex 17 of the Chicago Convention, quoted in [ICAODEFS]

Self-ID Message
[F3411-19] Message Type 3. Provides a 1 byte descriptor and 23 byte ASCII free text field, only. Expected to be used to provide context on the operation, e.g., mission intent.

SDO

SDSP
Supplemental Data Service Provider. An entity that participates in the UTM system, but provides services beyond those specified as basic UTM system functions (e.g., weather data). [FAACONOPS]

System Message
[F3411-19] Message Type 4. Provides general UAS information, including remote pilot location, multiple UA group operational area, etc.

U-space
EU concept and emerging framework for integration of UAS into all classes of airspace, specifically including high density urban areas, sharing airspace with manned aircraft [InitialView].

UA
Unmanned Aircraft. In popular parlance, "drone". "An aircraft which is intended to operate with no pilot on board" [ICAOUAS].

UAS
Unmanned Aircraft System. Composed of UA, all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and C2 links between UA and control station [F3411-19].

UAS ID
UAS identifier. Although called "UAS ID", it is actually unique to the UA, neither to the operator (as some UAS registration
numbers have been and for exclusively recreational purposes are continuing to be assigned), nor to the combination of GCS and UA that comprise the UAS. _Maximum length of 20 bytes_ [F3411-19]. If the UAS ID Type is 4, the proposed Specific Session ID, then the 20 bytes includes the subtype index, leaving only 19 bytes for the actual identifier.

**UAS ID Type**
UAS Identifier type index. 4 bits, see Section 3, Paragraph 6 for currently defined values 0-3. [F3411-19]

**UAS RID**
UAS Remote Identification and tracking. System to enable arbitrary Observers to identify UA during flight.

**USS**
UAS Service Supplier. "A USS is an entity that assists UAS Operators with meeting UTM operational requirements that enable safe and efficient use of airspace" and "... provide services to support the UAS community, to connect Operators and other entities to enable information flow across the USS Network, and to promote shared situational awareness among UTM participants" [FAACONOPS].

**UTM**
UAS Traffic Management. "A specific aspect of air traffic management which manages UAS operations safely, economically and efficiently through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions" [ICAOUTM]. In the US, according to the FAA, a "traffic management" ecosystem for "uncontrolled" low altitude UAS operations, separate from, but complementary to, the FAA’s ATC system for "controlled" operations of manned aircraft.

**V2V**
Vehicle-to-Vehicle. Originally communications between automobiles, now extended to apply to communications between vehicles generally. Often, together with Vehicle-to-Infrastructure (V2I) etc., generalized to V2X.

**VLOS**
Visual Line Of Sight. Typically used in describing operation of a UA by a "remote" pilot who can clearly directly (without video cameras or any aids other than glasses or under some rules binoculars) see the UA and its immediate flight environment. Potentially subject to blockage by foliage, structures, terrain, or other vehicles, more so than RF LOS.
3. UAS RID Problem Space

CAAs worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The US FAA has published a "final" rule [FRUR] and has described the key role that UAS RID plays in UAS Traffic Management (UTM) in [FAACONOPS] (especially Section 2.6). CAAs currently (2021) promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

The most widely cited such industry consensus technical standard for UAS RID is [F3411-19], which defines two means of UAS RID:

- **Network RID** defines a set of information for UAS to make available globally indirectly via the Internet, through servers that can be queried by Observers.

- **Broadcast RID** defines a set of messages for UA to transmit locally directly one-way over Bluetooth or Wi-Fi (without IP or any other protocols between the data link and application layers), to be received in real time by local Observers.

UAS using both means must send the same UAS RID application layer information via each [F3411-19]. The presentation may differ, as Network RID defines a data dictionary, whereas Broadcast RID defines message formats (which carry items from that same data dictionary). The interval (or rate) at which it is sent may differ, as Network RID can accommodate Observer queries asynchronous to UAS updates (which generally need be sent only when information, such as location, changes), whereas Broadcast RID depends upon Observers receiving UA messages at the time they are transmitted.

Network RID depends upon Internet connectivity in several segments from the UAS to each Observer. Broadcast RID should need Internet (or other Wide Area Network) connectivity only to retrieve UAS registry information using the directly locally received UAS Identifier (UAS ID) as the primary unique key for database lookup. Broadcast RID does not assume IP connectivity of UAS; messages are encapsulated by the UA _without IP_, directly in link layer frames (Bluetooth 4, Bluetooth 5, Wi-Fi NAN, IEEE 802.11 Beacon, or in the future perhaps others).

[F3411-19] specifies three UAS ID Type values and its currently (August 2021) proposed revision adds a fourth:
1 A static, manufacturer assigned, hardware serial number as defined in ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A].

2 A CAA assigned (generally static) ID, like the registration number of a manned aircraft.

3 A UTM system assigned UUID [RFC4122], which can but need not be dynamic.

4 A Specific Session ID, of any of an 8 bit range of subtypes defined external to ASTM and registered with ICAO, for which subtype 1 has been reserved by ASTM for the DRIP entity ID.

Per [Delegated], the EU allows only UAS ID Type 1. Under [FRUR], the US allows types 1 and 3. [NPRM] proposed that a type 3 "Session ID" would be "e.g., a randomly-generated alphanumeric code assigned by a Remote ID UAS Service Supplier (USS) on a per-flight basis designed to provide additional privacy to the operator", but given the omission of Network RID from [FRUR], how this is to be assigned in the US is still to be determined.

As yet apparently there are no CAA public proposals to use UAS ID Type 2. In the preamble of [FRUR], the FAA argues that registration numbers should not be sent in RID, insists that the capability of looking up registration numbers from information contained in RID should be restricted to FAA and other Government agencies, and implies that Session ID would be linked to the registration number only indirectly via the serial number in the registration database. The possibility of cryptographically blinding registration numbers, such that they can be revealed under specified circumstances, does not appear to be mentioned in applicable regulations or external technical standards.

Under [Delegated], the EU also requires an operator registration number (an additional identifier distinct from the UAS ID) that can be carried in an [F3411-19] optional Operator ID message.

[FRUR] allows RID requirements to be met by either the UA itself, which is then designated a "standard remote identification unmanned aircraft", or by an add-on "remote identification broadcast module". Relative to a standard RID UA, the different requirements for a module are that the latter: must transmit its own serial number (neither the serial number of the UA to which it is attached, nor a Session ID); must transmit takeoff location as a proxy for the location of the pilot/GCS; need not transmit UA emergency status; and is allowed to be used only for operations within VLOS of the remote pilot.
Jurisdictions may relax or waive RID requirements for certain operators and/or under certain conditions. For example, [FRUR] allows operators with UAS not equipped for RID to conduct VLOS operations at counter-intuitively named "FAA-recognized identification areas" (FRIA); radio controlled model aircraft flying clubs and other eligible organizations can apply to the FAA for such recognition of their operating areas.

3.1. Network RID

![Network RID Information Flow](image)

Figure 3: "Network RID Information Flow"

Figure 3 illustrates Network RID information flows. Only two of the three typically wireless links shown involving the UAS (UA-GCS, UA-Internet, and GCS-Internet) need exist to support C2 and Network RID. All three may exist, at the same or different times, especially in BVLOS operations. There must be some information flow path (direct or indirect) between the GCS and the UA, for the former to exercise C2 over the latter. If this path is two-way (as increasingly it is, even for inexpensive small UAS), the UA will also send its status (and position, if suitably equipped, e.g., with GNSS) to the GCS. There also must be some path between at least one subsystem of the UAS (UA or GCS) and the Internet, for the former to send status and position updates to its USS (serving _inter alia_ as a Net-RID SP).
Direct UA-Internet wireless links are expected to become more common, especially on larger UAS, but currently (2021) are rare. Instead, the RID data flow typically originates on the UA and passes through the GCS, or originates on the GCS. Network RID data makes three trips through the Internet (GCS-SP, SP-DP, DP-Observer, unless any of them are colocated), implying use of IP (and other middle layer protocols, e.g., TLS/TCP or DTLS/UDP) on those trips. IP is not necessarily used or supported on the UA-GCS link (if indeed that direct link exists, as it typically does now, but in BVLOS operations often will not).

Network RID is publish-subscribe-query. In the UTM context:

1. The UAS operator pushes an "operational intent" (the current term in UTM corresponding to a flight plan in manned aviation) to the USS (call it USS#1) that will serve that UAS (call it UAS#1) for that operation, primarily to enable deconfliction with other operations potentially impinging upon that operation’s 4-D airspace volume (call it Volume#1).

2. Assuming the operation is approved and commences, UAS#1 periodically pushes location/status updates to USS#1, which serves _inter alia_ as the Network RID Service Provider (Net-RID SP) for that operation.

3. When users of any other USS (whether they be other UAS operators or Observers) develop an interest in any 4-D airspace volume (e.g., because they wish to submit an operational intent or because they have observed a UA), they query their own USS on the volumes in which they are interested.

4. Their USS query, via the UTM Discovery and Synchronization Service (DSS), all other USS in the UTM system, and learn of any USS that have operations in those volumes (including any volumes intersecting them); thus those USS whose query volumes intersect Volume#1 (call them USS#2 through USS#n) learn that USS#1 has such operations.

5. Interested parties can then subscribe to track updates on that operation of UAS#1, via their own USS, which serve as Network RID Display Providers (Net-RID DP) for that operation.

6. USS#1 (as Net-RID SP) will then publish updates of UAS#1 status and position to all other subscribed USS in USS#2 through USS#n (as Net-RID DP).
7. All Net-RID DP subscribed to that operation of UAS#1 will deliver its track information to their users who subscribed to that operation of UAS#1 (via means unspecified by [F3411-19] etc., but generally presumed to be web browser based).

Network RID has several connectivity scenarios:

_Persistently Internet connected UA_ can consistently directly source RID information; this requires wireless coverage throughout the intended operational airspace volume, plus a buffer (e.g., winds may drive the UA out of the volume).

_Intermittently Internet connected UA_, can usually directly source RID information, but when offline (e.g., due to signal blockage by a large structure being inspected using the UAS), need the GCS to proxy source RID information.

_Indirectly connected UA_ lack the ability to send IP packets that will be forwarded into and across the Internet, but instead have some other form of communications to another node that can relay or proxy RID information to the Internet; typically this node would be the GCS (which to perform its function must know where the UA is, although C2 link outages do occur).

_Non-connected UA_ have no means of sourcing RID information, in which case the GCS or some other interface available to the operator must source it. In the extreme case, this could be the pilot or other agent of the operator using a web browser/application to designate, to a USS or other UTM entity, a time-bounded airspace volume in which an operation will be conducted. This is referred to as a "non-equipped network participant" engaging in "area operations". This may impede disambiguation of ID if multiple UAS operate in the same or overlapping 4-D volumes. In most airspace volumes, most classes of UA will not be permitted to fly if non-connected.

In most cases in the near term (2021), the Network RID first hop data link is likely to be cellular, which can also support BVLOS C2 over existing large coverage areas, or Wi-Fi, which can also support Broadcast RID. However, provided the data link can support at least UDP/IP and ideally also TCP/IP, its type is generally immaterial to higher layer protocols. The UAS, as the ultimate source of Network RID information, feeds a Net-RID SP (typically the USS to which the UAS operator subscribes), which proxies for the UAS and other data sources. An Observer or other ultimate consumer of Network RID information obtains it from a Net-RID DP (also typically a USS), which aggregates information from multiple Net-RID SPs to offer airspace Situational Awareness (SA) coverage of a volume of interest.
Network RID Service and Display providers are expected to be implemented as servers in well-connected infrastructure, communicating with each other via the Internet, and accessible by Observers via means such as web Application Programming Interfaces (APIs) and browsers.

Network RID is the less constrained of the defined UAS RID means. [F3411-19] specifies only Net-RID SP to Net-RID DP information exchanges. It is presumed that IETF efforts supporting the more constrained Broadcast RID (see next section) can be generalized for Network RID and potentially also for UAS to USS or other UTM communications.

3.2. Broadcast RID

```
+-------------------+    +-------------------+
| Unmanned Aircraft |    | Observer’s device (e.g., smartphone) |
|                  +-------------------+    +-------------------+
        v                      v
    +-------------o-------------+
    | app messages directly over one-way RF data link |
```

Figure 4: "Broadcast RID Information Flow"

Figure 4 illustrates Broadcast RID information flow. Note the absence of the Internet from the figure. This is because Broadcast RID is one-way direct transmission of application layer messages over a RF data link (without IP) from the UA to local Observer devices. Internet connectivity is involved only in what the Observer chooses to do with the information received, such as verify signatures using a web-based Broadcast Authentication Verifier Service and look up information in registries using the UAS ID as the primary unique key.

Broadcast RID is conceptually similar to Automatic Dependent Surveillance - Broadcast (ADS-B). However, for various technical and other reasons, regulators including the EASA have not indicated intent to allow, and FAA has explicitly prohibited, use of ADS-B for UAS RID.
[F3411-19] specifies four Broadcast RID data links: Bluetooth 4.x, Bluetooth 5.x with Extended Advertisements and Long Range Coded PHY (S=8), Wi-Fi NAN at 2.4 GHz, and Wi-Fi NAN at 5 GHz. A UA must broadcast (using advertisement mechanisms where no other option supports broadcast) on at least one of these. If sending on Bluetooth 5.x, it is also required concurrently to do so on 4.x (referred to in [F3411-19] as Bluetooth Legacy); current (2021) discussions in ASTM F38.02 on revising the standard, motivated by European standards drafts, suggest that both Bluetooth versions will be required. If broadcasting Wi-Fi NAN at 5 GHz, it is also required concurrently to do so at 2.4 GHz; current discussions in F38.02 include relaxing this. Wi-Fi Beacons are also under consideration. Future revisions of [F3411-19] may allow other data links.

The selection of the Broadcast media was driven by research into what is commonly available on ‘ground’ units (smartphones and tablets) and what was found as prevalent or ‘affordable’ in UA. Further, there must be an API for the Observer’s receiving application to have access to these messages. As yet only Bluetooth 4.x support is readily available, thus the current focus is on working within the 31 byte payload limit of the Bluetooth 4.x "Broadcast Frame" transmitted as an "advertisement" on beacon channels. After overheads, this limits the RID message to 25 bytes and UAS ID string to a maximum length of 20 bytes.

Length constraints also preclude a single Bluetooth 4.x frame carrying not only the UAS ID but also position, velocity, and other information that should be bound to the UAS ID, much less strong authentication data. Messages that cannot be encapsulated in a single frame (thus far, only the Authentication Message) must be segmented into message "pages" (in the terminology of [F3411-19]). Message pages must somehow be correlated as belonging to the same message. Messages carrying position, velocity and other data must somehow be correlated with the Basic ID message that carries the UAS ID. This correlation is expected to be done on the basis of MAC address: this may be complicated by MAC address randomization; not all the common devices expected to be used by Observers have APIs that make sender MAC addresses available to user space receiver applications; and MAC addresses are easily spoofed. Data elements are not so detached on other media (see Message Pack in the paragraph after next).
Broadcast RID specifies several message types. The 4 bit message type field in the header can index up to 16 types. Only 7 are currently defined. Only 2 are mandatory. All others are optional, unless required by a jurisdictional authority, e.g., a CAA. To satisfy both EASA and FAA rules, all types are needed, except Self-ID and Authentication, as the data elements required by the rules are scattered across several message types (along with some data elements not required by the rules).

The Message Pack (type 0xF) is not actually a message, but the framed concatenation of at most one message of each type of any subset of the other types, in type index order. Some of the messages that it can encapsulate are mandatory, others optional. The Message Pack itself is mandatory on data links that can encapsulate it in a single frame (Bluetooth 5.x and Wi-Fi).

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Req</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>Basic ID</td>
<td>Mandatory</td>
<td>-</td>
</tr>
<tr>
<td>0x1</td>
<td>Location/Vector</td>
<td>Mandatory</td>
<td>-</td>
</tr>
<tr>
<td>0x2</td>
<td>Authentication</td>
<td>Optional</td>
<td>paged</td>
</tr>
<tr>
<td>0x3</td>
<td>Self-ID</td>
<td>Optional</td>
<td>free text</td>
</tr>
<tr>
<td>0x4</td>
<td>System</td>
<td>Optional</td>
<td>-</td>
</tr>
<tr>
<td>0x5</td>
<td>Operator</td>
<td>Optional</td>
<td>-</td>
</tr>
<tr>
<td>0xF</td>
<td>Message Pack</td>
<td>-</td>
<td>BT5 and Wi-Fi</td>
</tr>
</tbody>
</table>

See Section 5.4.5 and Table 3 of [F3411-19]

Table 1: F3411-19 Message Types

Broadcast RID specifies very few quantitative performance requirements: static information must be transmitted at least once per 3 seconds; dynamic information (the Location/Vector message) must be transmitted at least once per second and be no older than one second when sent. [FRUR] requires all information be sent at least once per second.
[F3411-19] Broadcast RID transmits all information as cleartext (ASCII or binary), so static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g., package delivery routes of competitors.

Any UA can assert any ID using the [F3411-19] required Basic ID message, which lacks any provisions for verification. The Position/Vector message likewise lacks provisions for verification, and does not contain the ID, so must be correlated somehow with a Basic ID message: the developers of [F3411-19] have suggested using the MAC addresses on the Broadcast RID data link, but these may be randomized by the operating system stack to avoid the adversarial correlation problems of static identifiers.

The [F3411-19] optional Authentication Message specifies framing for authentication data, but does not specify any authentication method, and the maximum length of the specified framing is too short for conventional digital signatures and far too short for conventional certificates (e.g., X.509). Fetching certificates via the Internet is not always possible (e.g., Observers working in remote areas, such as national forests), so devising a scheme whereby certificates can be transported over Broadcast RID is necessary. The one-way nature of Broadcast RID precludes challenge-response security protocols (e.g., Observers sending nonces to UA, to be returned in signed messages). Without DRIP extensions to [F3411-19], an Observer would be seriously challenged to validate the asserted UAS ID or any other information about the UAS or its operator looked up therefrom.

In the currently (2021) proposed revision to ASTM [F3411-19], a new Authentication Type 5 has been defined, "Specific Authentication Method" (SAM), to enable SDOs other than ASTM to define authentication payload formats. The first byte of the payload is the SAM Type, used to demultiplex such variant formats. All formats for other than private experimental use must be registered with ICAO, which assigns the SAM Type. Any authentication message payload that is to be sent in exactly the same form over all currently specified Broadcast RID media is limited by lower layer constraints to a total length of 201 bytes. For Authentication Type 5, expected to be used by DRIP, the SAM Type byte consumes the first of these, limiting DRIP authentication payload formats to a maximum of 200 bytes.
3.3. USS in UTM and RID

UAS RID and UTM are complementary; Network RID is a UTM service. The backbone of the UTM system is comprised of multiple USS: one or several per jurisdiction; some limited to a single jurisdiction, others spanning multiple jurisdictions. USS also serve as the principal or perhaps the sole interface for operators and UAS into the UTM environment. Each operator subscribes to at least one USS. Each UAS is registered by its operator in at least one USS. Each operational intent is submitted to one USS; if approved, that UAS and operator can commence that operation. During the operation, status and location of that UAS must be reported to that USS, which in turn provides information as needed about that operator, UAS, and operation into the UTM system and to Observers via Network RID.

USS provide services not limited to Network RID; indeed, the primary USS function is deconfliction of airspace usage by different UAS and other (e.g., manned aircraft, rocket launch) operations. Most deconfliction involving a given operation is hoped to be completed prior to commencing that operation, and is called "strategic deconfliction". If that fails, "tactical deconfliction" comes into play; ABDAA may not involve USS, but GBDAA likely will. Dynamic constraints, formerly called UAS Volume Restrictions (UVR), can be necessitated by local emergencies, extreme weather, etc., specified by authorities on the ground, and propagated in UTM.

No role for USS in Broadcast RID is currently specified by regulators or [F3411-19]. However, USS are likely to serve as registries (or perhaps registrars) for UAS (and perhaps operators); if so, USS will have a role in all forms of RID. Supplemental Data Service Providers (SDSP) are also likely to find roles, not only in UTM as such but also in enhancing UAS RID and related services. Whether USS, SDSP, etc. are involved or not, RID services, narrowly defined, provide regulator specified identification information; more broadly defined, RID services may leverage identification to facilitate related services or functions, likely beginning with V2X.

3.4. DRIP Focus

In addition to the gaps described above, there is a fundamental gap in almost all current or proposed regulations and technical standards for UAS RID. As noted above, ID is not an end in itself, but a means. Protocols specified in [F3411-19] etc. provide limited information potentially enabling, and no technical means for, an Observer to communicate with the pilot, e.g., to request further information on the UAS operation or exit from an airspace volume in an emergency. The System Message provides the location of the pilot/GCS, so an Observer could physically go to the asserted location to
look for the remote pilot; this is at best slow and may not be feasible. What if the pilot is on the opposite rim of a canyon, or there are multiple UAS operators to contact, whose GCS all lie in different directions from the Observer? An Observer with Internet connectivity and access privileges could look up operator PII in a registry, then call a phone number in hopes someone who can immediately influence the UAS operation will answer promptly during that operation; this is at best unreliable and may not be prudent. Should pilots be encouraged to answer phone calls while flying? Internet technologies can do much better than this.

Thus complementing [F3411-19] with protocols enabling strong authentication, preserving operator privacy while enabling immediate use of information by authorized parties, is critical to achieve widespread adoption of a RID system supporting safe and secure operation of UAS. Just as [F3411-19] is expected to be approved by regulators as a basic means of compliance with UAS RID regulations, DRIP is expected likewise to be approved to address further issues, starting with the creation and registration of Session IDs.

DRIP will focus on making information obtained via UAS RID immediately usable:

1. by making it trustworthy (despite the severe constraints of Broadcast RID);

2. by enabling verification that a UAS is registered for RID, and if so, in which registry (for classification of trusted operators on the basis of known registry vetting, even by Observers lacking Internet connectivity at observation time);

3. by facilitating independent reports of UA aeronautical data (location, velocity, etc.) to confirm or refute the operator self-reports upon which UAS RID and UTM tracking are based;

4. by enabling instant establishment, by authorized parties, of secure communications with the remote pilot.

The foregoing considerations, beyond those addressed by baseline UAS RID standards such as [F3411-19], imply the following requirements for DRIP.
4. Requirements

The following requirements apply to DRIP as a set of related protocols, various subsets of which, in conjunction with other IETF and external technical standards, may suffice to comply with the regulations in any given jurisdiction or meet any given user need. It is not intended that each and every DRIP protocol alone satisfy each and every requirement. To satisfy these requirements, Internet connectivity is required some of the time: e.g., to support DRIP entity identifier creation/registration; but not all of the time, e.g., authentication of an asserted DRIP entity identifier can be achieved by a fully working and provisioned Observer device even when that device is off-line so is required at all times.

4.1. General

4.1.1. Normative Requirements

GEN-1 Provable Ownership: DRIP MUST enable verification that the asserted entity (typically UAS) ID is that of the actual current sender (i.e., the entity ID in the DRIP authenticated message set is not a replay attack or other spoof, e.g., by verifying an asymmetric cryptographic signature using a sender provided public key from which the asserted UAS ID can be at least partially derived), even on an Observer device lacking Internet connectivity at the time of observation.

GEN-2 Provable Binding: DRIP MUST enable the cryptographic binding of all other [F3411-19] messages from the same actual current sender to the UAS ID asserted in the Basic ID message.

GEN-3 Provable Registration: DRIP MUST enable cryptographically secure verification that the UAS ID is in a registry and identification of that registry, even on an Observer device lacking Internet connectivity at the time of observation; the same sender may have multiple IDs, potentially in different registries, but each ID must clearly indicate in which registry it can be found.

GEN-4 Readability: DRIP MUST enable information (regulation required elements, whether sent via UAS RID or looked up in registries) to be read and utilized by both humans and software.
Gateway: DRIP MUST enable Broadcast RID to Network RID application layer gateways to stamp messages with precise date/time received and receiver location, then relay them to a network service (e.g., SDSP or distributed ledger) whenever the gateway has Internet connectivity.

Contact: DRIP MUST enable dynamically establishing, with AAA, per policy, strongly mutually authenticated, end-to-end strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including at least the pilot (remote pilot or Pilot In Command), the USS (if any) under which the operation is being conducted, and registries in which data on the UA and pilot are held, whenever each party to such desired communications has a currently usable means of resolving the other party’s DRIP entity identifier to a locator (IP address) and currently usable bidirectional IP (not necessarily Internet) connectivity with the other party.

QoS: DRIP MUST enable policy based specification of performance and reliability parameters.

Mobility: DRIP MUST support physical and logical mobility of UA, GCS and Observers. DRIP SHOULD support mobility of essentially all participating nodes (UA, GCS, Observers, Net-RID SP, Net-RID DP, Private Registry, SDSP, and potentially others as RID and UTM evolve).

Multihoming: DRIP MUST support multihoming of UA and GCS, for make-before-break smooth handoff and resiliency against path/link failure. DRIP SHOULD support multihoming of essentially all participating nodes.

Multicast: DRIP SHOULD support multicast for efficient and flexible publish-subscribe notifications, e.g., of UAS reporting positions in designated airspace volumes.

Management: DRIP SHOULD support monitoring of the health and coverage of Broadcast and Network RID services.

4.1.2. Rationale

Requirements imposed either by regulation or [F3411-19] are not reiterated here, but drive many of the numbered requirements listed here. The [FRUR] regulatory QoS requirement currently would be satisfied by ensuring information refresh rates of at least 1 Hertz, with latencies no greater than 1 second, at least 80% of the time, but these numbers may vary between jurisdictions and over time. So
instead the DRIP QoS requirement is that performance, reliability, etc. parameters be user policy specifiable, which does not imply satisfiable in all cases, but (especially together with the management requirement) implies that when specifications are not met, appropriate parties are notified.

The "provable ownership" requirement addresses the possibility that the actual sender is not the claimed sender (i.e., is a spoofer). The "provable binding" requirement addresses the MAC address correlation problem of [F3411-19] noted above. The "provable registration" requirement may impose burdens not only on the UAS sender and the Observer’s receiver, but also on the registry; yet it cannot depend upon the Observer being able to contact the registry at the time of observing the UA. The "readability" requirement pertains to the structure and format of information at endpoints rather than its encoding in transit, so may involve machine assisted format conversions, e.g., from binary encodings, and/or decryption (see Section 4.3).

The "gateway" requirement is in pursuit of three objectives: (1) mark up a RID message with where and when it was actually received, which may agree or disagree with the self-report in the set of messages; (2) defend against replay attacks; and (3) support optional SDSP services such as multilateration, to complement UAS position self-reports with independent measurements. This is the only instance in which DRIP transports [F3411-19] messages; most of DRIP pertains to the authentication of such messages and identifiers carried in them.

The "contact" requirement allows any party that learns a UAS ID (that is a DRIP entity identifier rather than another UAS ID Type) to request establishment of a communications session with the corresponding UAS RID sender and certain entities associated with that UAS, but AAA and policy restrictions, inter alia, on resolving the identifier to any locators (typically IP addresses), should prevent unauthorized parties from distracting or harassing pilots. Thus some but not all Observers of UA, receivers of Broadcast RID, clients of Network RID, and other parties can become successfully initiating endpoints for these sessions.
The "QoS" requirement is only that performance and reliability parameters can be _specified_ by policy, not that any such specifications must be guaranteed to be met; any failure to meet such would be reported under the "management" requirement. Examples of such parameters are the maximum time interval at which messages carrying required data elements may be transmitted, the maximum tolerable rate of loss of such messages, and the maximum tolerable latency between a dynamic data element (e.g., GNSS position of UA) being provided to the DRIP sender and that element being delivered by the DRIP receiver to an application.

The "mobility" requirement refers to rapid geographic mobility of nodes, changes of their points of attachment to networks, and changes to their IP addresses; it is not limited to micro-mobility within a small geographic area or single Internet access provider.

4.2. Identifier

4.2.1. Normative Requirements

ID-1 Length: The DRIP entity identifier MUST NOT be longer than 19 bytes, to fit in the Specific Session ID subfield of the UAS ID field of the Basic ID message of the currently (August 2021) proposed revision of [F3411-19].

ID-2 Registry ID: The DRIP identifier MUST be sufficient to identify a registry in which the entity identified therewith is listed.

ID-3 Entity ID: The DRIP identifier MUST be sufficient to enable lookups of other data associated with the entity identified therewith in that registry.

ID-4 Uniqueness: The DRIP identifier MUST be unique within the applicable global identifier space from when it is first registered therein until it is explicitly de-registered therefrom (due to, e.g., expiration after a specified lifetime, revocation by the registry, or surrender by the operator).

ID-5 Non-spoofability: The DRIP identifier MUST NOT be spoofable within the context of a minimal Remote ID broadcast message set (to be specified within DRIP to be sufficient collectively to prove sender ownership of the claimed identifier).

ID-6 Unlinkability: The DRIP identifier MUST NOT facilitate adversarial correlation over multiple operations. If this is accomplished by limiting each identifier to a single use or brief period of usage, the DRIP identifier MUST support well-defined, scalable, timely registration methods.
4.2.2. Rationale

The DRIP identifier can refer to various entities. In the primary initial use case, the entity to be identified is the UA. Entities to be identified in other likely use cases include but are not limited to the operator, USS, and Observer. In all cases, the entity identified must own (have the exclusive capability to use, such that receivers can verify its ownership of) the identifier.

The DRIP identifier can be used at various layers. In Broadcast RID, it would be used by the application running directly over the data link. In Network RID, it would be used by the application running over HTTPS (not required by DRIP but generally used by Network RID implementations) and possibly other protocols. In RID initiated V2X applications such as DAA and C2, it could be used between the network and transport layers, e.g., with the Host Identity Protocol (HIP, [RFC9063], [RFC7401], etc.), or between the transport and application layers, e.g., with Datagram Transport Layer Security (DTLS, [RFC6347]).

Registry ID (which registry the entity is in) and Entity ID (which entity it is, within that registry) are requirements on a single DRIP entity identifier, not separate (types of) ID. In the most common use case, the entity will be the UA, and the DRIP identifier will be the UAS ID; however, other entities may also benefit from having DRIP identifiers, so the entity type is not prescribed here.

Whether a UAS ID is generated by the operator, GCS, UA, USS, registry, or some collaboration thereamong, is unspecified; however, there must be agreement on the UAS ID among these entities. Management of DRIP identifiers is the primary function of their registration hierarchies, from the root (presumably IANA), through sector-specific and regional authorities (presumably ICAO and CAAs), to the identified entities themselves.

While "uniqueness" might be considered an implicit requirement for any identifier, here the point of the explicit requirement is not just that it should be unique, but also where and when it should be unique: global scope within a specified space, from registration to deregistration.

While "non-spoofability" imposes requirements for and on a DRIP authentication protocol, it also imposes requirements on the properties of the identifier itself. An example of how the nature of the identifier can support non-spoofability is embedding a hash of both the registry ID and a public key of the entity in the entity identifier, thus making it self-authenticating any time the entity’s corresponding private key is used to sign a message.
While "unlinkability" is a privacy desideratum (see next section), it imposes requirements on the DRIP identifier itself, as distinct from other currently permitted choices for the UAS ID (including primarily the static serial number of the UA or RID module).

4.3. Privacy

4.3.1. Normative Requirements

PRIV-1 Confidential Handling: DRIP MUST enable confidential handling of private information (i.e., any and all information designated by neither cognizant authority nor the information owner as public, e.g., personal data).

PRIV-2 Encrypted Transport: DRIP MUST enable selective strong encryption of private data in motion in such a manner that only authorized actors can recover it. If transport is via IP, then encryption MUST be end-to-end, at or above the IP layer. DRIP MUST NOT encrypt safety critical data to be transmitted over Broadcast RID in any situation where it is unlikely that local Observers authorized to access the plaintext will be able to decrypt it or obtain it from a service able to decrypt it. DRIP MUST NOT encrypt data when/where doing so would conflict with applicable regulations or CAA policies/procedures, i.e., DRIP MUST support configurable disabling of encryption.

PRIV-3 Encrypted Storage: DRIP SHOULD facilitate selective strong encryption of private data at rest in such a manner that only authorized actors can recover it.

PRIV-4 Public/Private Designation: DRIP SHOULD facilitate designation, by cognizant authorities and information owners, of which information is public and which is private. By default, all information required to be transmitted via Broadcast RID, even when actually sent via Network RID or stored in registries, is assumed to be public; all other information held in registries for lookup using the UAS ID is assumed to be private.

PRIV-5 Pseudonymous Rendezvous: DRIP MAY enable mutual discovery of and communications among participating UAS operators whose UA are in 4-D proximity, using the UAS ID without revealing pilot/operator identity or physical location.
4.3.2. Rationale

Most data to be sent via Broadcast RID or Network RID is public, thus the "encrypted transport" requirement for private data is selective, e.g., for the entire payload of the Operator ID Message, but only the pilot/GCS location fields of the System Message. Safety critical data includes at least the UA location. Other data also may be deemed safety critical, e.g., in some jurisdictions the pilot/GCS location is implied to be safety critical.

UAS have several potential means of assessing the likelihood that local Observers authorized to access the plaintext will be able to decrypt it or obtain it from a service able to decrypt it. If the UAS is not participating in UTM, an Observer would have no means of obtaining a decryption key or decryption services from a cognizant USS. If the UAS is participating in UTM, but has lost connectivity with its USS, then an Observer within visual LOS of the UA is also unlikely to be able to communicate with that USS (whether due to the USS being offline or the UAS and Observer being in an area with poor Internet connectivity). Either of these conditions (UTM non-participation or USS unreachability) would be known to the UAS.

In some jurisdictions, the configurable enabling and disabling of encryption may need to be outside the control of the operator. [FRUR] mandates manufacturers design RID equipment with some degree of tamper resistance; the preamble and other FAA commentary suggest this is to reduce the likelihood that an operator, intentionally or unintentionally, might alter the values of the required data elements or disable their transmission in the required manner (e.g., as cleartext).

How information is stored on end systems is out of scope for DRIP. Encouraging privacy best practices, including end system storage encryption, by facilitating it with protocol design reflecting such considerations, is in scope. Similar logic applies to methods for designating information as public or private.

The privacy requirements above are for DRIP, neither for [F3411-19] (which requires obfuscation of location to any Network RID subscriber engaging in wide area surveillance, limits data retention periods, etc., in the interests of privacy), nor for UAS RID in any specific jurisdiction (which may have its own regulatory requirements). The requirements above are also in a sense parameterized: who are the "authorized actors", how are they designated, how are they authenticated, etc.?

4.4. Registries
4.4.1. Normative Requirements

REG-1 Public Lookup: DRIP MUST enable lookup, from the UAS ID, of information designated by cognizant authority as public, and MUST NOT restrict access to this information based on identity or role of the party submitting the query.

REG-2 Private Lookup: DRIP MUST enable lookup of private information (i.e., any and all information in a registry, associated with the UAS ID, that is designated by neither cognizant authority nor the information owner as public), and MUST, according to applicable policy, enforce AAA, including restriction of access to this information based on identity or role of the party submitting the query.

REG-3 Provisioning: DRIP MUST enable provisioning registries with static information on the UAS and its operator, dynamic information on its current operation within the U-space/UTM (including means by which the USS under which the UAS is operating may be contacted for further, typically even more dynamic, information), and Internet direct contact information for services related to the foregoing.

REG-4 AAA Policy: DRIP AAA MUST be specifiable by policies; the definitive copies of those policies must be accessible in registries; administration of those policies and all DRIP registries must be protected by AAA.

4.4.2. Rationale

Registries are fundamental to RID. Only very limited information can be Broadcast, but extended information is sometimes needed. The most essential element of information sent is the UAS ID itself, the unique key for lookup of extended information in registries. Beyond designating the UAS ID as that unique key, the registry information model is not specified herein, in part because regulatory requirements for different registries (UAS operators and their UA, each narrowly for UAS RID and broadly for U-space/UTM) and business models for meeting those requirements are in flux. While it is expected that registry functions will be integrated with USS, who will provide them is not yet determined in most, and is expected to vary between, jurisdictions. However this evolves, the essential registry functions, starting with management of identifiers, are expected to remain the same, so are specified herein.

While most data to be sent via Broadcast or Network RID is public, much of the extended information in registries will be private. Thus AAA for registries is essential, not just to ensure that access is
Internet-Draft              DRIP Requirements             September 2021

... granted only to strongly authenticated, duly authorized parties, but also to support subsequent attribution of any leaks, audit of who accessed information when and for what purpose, etc. As specific AAA requirements will vary by jurisdictional regulation, provider philosophy, customer demand, etc., they are left to specification in policies, which should be human readable to facilitate analysis and discussion, and machine readable to enable automated enforcement, using a language amenable to both, e.g., XACML.

The intent of the negative and positive access control requirements on registries is to ensure that no member of the public would be hindered from accessing public information, while only duly authorized parties would be enabled to access private information. Mitigation of Denial of Service attacks and refusal to allow database mass scraping would be based on those behaviors, not on identity or role of the party submitting the query _per se_, but querant identity information might be gathered (by security systems protecting DRIP implementations) on such misbehavior.

By "Internet direct contact information" is meant a locator (e.g., IP address), or identifier (e.g., FQDN) that can be resolved to a locator, which would enable initiation of an end-to-end communication session using a well known protocol (e.g., SIP).

5. IANA Considerations

This document does not make any IANA request.

6. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. This document does not define any protocols, so security considerations of such are speculative. Potential vulnerabilities of DRIP solutions to these requirements include but are not limited to:

* Sybil attacks

* confusion created by many spoofed unsigned messages

* processing overload induced by attempting to verify many spoofed signed messages (where verification will fail but still consume cycles)

* malicious or malfunctioning registries

* interception by on-path attacker of (i.e., Man In The Middle attacks on) registration messages

* UA impersonation through private key extraction, improper key sharing, or carriage of a small (presumably harmless) UA, i.e., as a "false flag", by a larger (malicious) UA

It may be inferred from the general requirements (Section 4.1) for provable ownership, provable binding, and provable registration, together with the identifier requirements (Section 4.2), that DRIP must provide:

* message integrity
* non-repudiation
* defense against replay attacks
* defense against spoofing

One approach to so doing involves verifiably binding the DRIP identifier to a public key. Providing these security features, whether via this approach or another, is likely to be especially challenging for Observers without Internet connectivity at the time of observation. For example, checking the signature of a registry on a public key certificate received via Broadcast RID in a remote area presumably would require that the registry’s public key had been previously installed on the Observer’s device, yet there may be many registries and the Observer’s device may be storage constrained, and new registries may come on-line subsequent to installation of DRIP software on the Observer’s device. See also Figure 1 and the associated explanatory text, especially the second paragraph after the figure. Thus there may be caveats on the extent to which requirements can be satisfied in such cases, yet strenuous effort should be made to satisfy them, as such cases, e.g., firefighting in a national forest, are important. Each numbered requirement _a priori_ expected to suffer from such limitations (General requirements for Gateway and Contact functionality) contains language stating when it applies.

7. Privacy and Transparency Considerations

Privacy and transparency are important for legal reasons including regulatory consistency. [EU2018] states "harmonised and interoperable national registration systems... should comply with the applicable Union and national law on privacy and processing of personal data, and the information stored in those registration systems should be easily accessible."
Privacy and transparency (where essential to security or safety) are also ethical and moral imperatives. Even in cases where old practices (e.g., automobile registration plates) could be imitated, when new applications involving PII (such as UAS RID) are addressed and newer technologies could enable improving privacy, such opportunities should not be squandered. Thus it is recommended that all DRIP work give due regard to [RFC6973] and more broadly [RFC8280].

However, privacy and transparency are often conflicting goals, demanding careful attention to their balance.

DRIP information falls into two classes: that which, to achieve the purpose, must be published openly as cleartext, for the benefit of any Observer (e.g., the basic UAS ID itself); and that which must be protected (e.g., PII of pilots) but made available to properly authorized parties (e.g., public safety personnel who urgently need to contact pilots in emergencies).

How properly authorized parties are authorized, authenticated, etc. are questions that extend beyond the scope of DRIP, but DRIP may be able to provide support for such processes. Classification of information as public or private must be made explicit and reflected with markings, design, etc. Classifying the information will be addressed primarily in external standards; herein it will be regarded as a matter for CAA, registry, and operator policies, for which enforcement mechanisms will be defined within the scope of DRIP WG and offered. Details of the protection mechanisms will be provided in other DRIP documents. Mitigation of adversarial correlation will also be addressed.

8. References

8.1. Normative References


8.2. Informative References


[FAACONOPS]

[FR24]

[FRUR]

[GDPR]

[I-D.ietf-raw-ldacs]

[ICAOATM]

[ICAODEFS]

[ICAOUAS]

[ICAOOUTM]


Appendix A. Discussion and Limitations

This document is largely based on the process of one SDO, ASTM. Therefore, it is tailored to specific needs and data formats of this standard. Other organizations, for example in EU, do not necessarily follow the same architecture.

The need for drone ID and operator privacy is an open discussion topic. For instance, in the ground vehicular domain each car carries a publicly visible plate number. In some countries, for nominal cost or even for free, anyone can resolve the identity and contact information of the owner. Civil commercial aviation and maritime industries also have a tradition of broadcasting plane or ship ID, coordinates, and even flight plans in plain text. Community networks such as OpenSky [OpenSky] and Flightradar24 [FR24] use this open information through ADS-B to deploy public services of flight tracking. Many researchers also use these data to perform optimization of routes and airport operations. Such ID information should be integrity protected, but not necessarily confidential.

In civil aviation, aircraft identity is broadcast by a device known as transponder. It transmits a four octal digit squawk code, which is assigned by a traffic controller to an airplane after approving a flight plan. There are several reserved codes such as 7600 which indicate radio communication failure. The codes are unique in each traffic area and can be re-assigned when entering another control area. The code is transmitted in plain text by the transponder and also used for collision avoidance by a system known as Traffic alert and Collision Avoidance System (TCAS). The system could be used for UAS as well initially, but the code space is quite limited and likely to be exhausted soon. The number of UAS far exceeds the number of civil airplanes in operation.

The ADS-B system is utilized in civil aviation for each "ADS-B Out" equipped airplane to broadcast its ID, coordinates, and altitude for other airplanes and ground control stations. If this system is adopted for drone IDs, it has additional benefit with backward compatibility with civil aviation infrastructure; then, pilots and dispatchers will be able to see UA on their control screens and take those into account. If not, a gateway translation system between the proposed drone ID and civil aviation system should be implemented. Again, system saturation due to large numbers of UAS is a concern.

The Mode S transponders used in all TCAS and most ADS-B Out installations are assigned an ICAO 24 bit "address" (arguably really an identifier rather than a locator) that is associated with the aircraft as part of its registration. In the US alone, well over $2^{20}$ UAS are already flying; thus, a 24 bit space likely would be
rapidly exhausted if used for UAS (other than large UAS flying in controlled airspace, especially internationally, under rules other than those governing small UAS at low altitudes).

Wi-Fi and Bluetooth are two wireless technologies currently recommended by ASTM specifications due to their widespread use and broadcast nature. However, those have limited range (max 100s of meters) and may not reliably deliver UAS ID at high altitude or distance. Therefore, a study should be made of alternative technologies from the telecom domain (WiMAX / IEEE 802.16, 5G) or sensor networks (Sigfox, LoRa). Such transmission technologies can impose additional restrictions on packet sizes and frequency of transmissions, but could provide better energy efficiency and range.

In civil aviation, Controller-Pilot Data Link Communications (CPDLC) is used to transmit command and control between the pilots and ATC. It could be considered for UAS as well due to long range and proven use despite its lack of security [CPDLC].

L-band Digital Aeronautical Communications System (LDACS) is being standardized by ICAO and IETF for use in future civil aviation [I-D.ietf-raw-ldacs]. It provides secure communication, positioning, and control for aircraft using a dedicated radio band. It should be analyzed as a potential provider for UAS RID as well. This will bring the benefit of a global integrated system creating a global airspace use awareness.

Acknowledgments

The work of the FAA’s UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM [F3411-19] and IETF DRIP efforts. The work of Gabriel Cox, Intel Corp., and their Open Drone ID collaborators opened UAS RID to a wider community. 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 extensively reviewed or otherwise contributed to this document include Amelia Andersdotter, Carsten Bormann, Toerless Eckert, Susan Hares, Mika Jarvenpaa, Alexandre Petrescu, Saulo Da Silva and Shuai Zhao. Thanks to Linda Dunbar for the Secdir review, Nagendra Nainar for the Opsdir review and Suresh Krishnan for the Gen-ART review. Thanks to IESG members Roman Danyliw, Erik Kline, Murray Kucherawy and Robert Wilton for helpful and positive comments. Thanks to chairs Daniel Migault and Mohamed Boucadair for direction of our team of authors and editor, some of whom are newcomers to writing IETF documents. Thanks especially to Internet Area Director Eric Vyncke for guidance and support.
Authors’ Addresses

Stuart W. Card (editor)
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

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping
Sweden

Email: gurtov@acm.org
Abstract

This document describes using the ASTM Broadcast Remote ID (B-RID) specification in a "crowd sourced" smart phone environment to provide much of the ASTM and FAA envisioned Network Remote ID (Net-RID) functionality. This crowd sourced B-RID (CS-RID) data will use multilateration to add a level of reliability in the location data on the Unmanned Aircraft (UA). The crowd sourced environment will also provide a monitoring coverage map to authorized observers.

Status of This Memo

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

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

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

This Internet-Draft will expire on 11 November 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.  Introduction ................................................. 3
   1.1. Role of Supplemental Data Service Provider (SDSP) .......... 4
   1.2. Draft Status ........................................... 4
2.  Terms and Definitions ........................................ 4
   2.1. Requirements Terminology ................................ 5
   2.2. Definitions ............................................. 5
3.  Problem Space ................................................ 5
   3.1. Meeting the needs of Network Remote ID ..................... 5
   3.2. Advantages of Broadcast Remote ID ........................ 6
   3.3. Trustworthiness of Proxyed Data .......................... 6
   3.4. Defense against fraudulent RID Messages ................... 6
4.  The Finder - SDSP Security Relationship ......................... 6
   4.1. SDSP Heartbeats ......................................... 7
   4.2. The Finder Map ......................................... 7
   4.3. Managing Finders ......................................... 8
5.  UA location via multilateration ................................ 8
   5.1. GPS Inaccuracy ......................................... 8
6.  The CS-RID Messages ........................................... 9
   6.1. CS-RID MESSAGE TYPE ...................................... 9
      6.1.1. CDDL description for CS-RID message type ............... 10
   6.2. The CS-RID B-RID Proxy Message .......................... 11
      6.2.1. CS-RID ID ........................................... 12
      6.2.2. CDDL description for CS-RID B-RID Proxy Message ...... 12
   6.3. CS-RID Finder Registration ............................... 13
      6.3.1. CDDL description for Finder Registration .............. 13
   6.4. CS-RID SDSP Response ..................................... 14
      6.4.1. CDDL description for SDSP Response ..................... 14
   6.5. CS-RID Location Update ................................... 15
      6.5.1. CDDL description for Location Update .................. 15
   6.6. SDSP Heartbeat .......................................... 15
      6.6.1. CDDL description for SDSP Heartbeat ................... 16
7.  The Full CS-RID CDDL specification ............................ 16
8.  IANA Considerations ........................................... 19
9.  Security Considerations ....................................... 19
   9.1. Privacy Concerns ........................................ 19
10. References .................................................... 19
    10.1. Normative References ................................... 19
1. Introduction

This document defines a mechanism to capture the ASTM Broadcast Remote ID messages (B-RID) [F3411-19] on any Internet connected device that receives them and can forward them to the Supplemental Data Service Providers (SDSPs) responsible for the geographic area the UA and receivers are in. This will create a ecosystem that will meet most if not all data collection requirements that Civil Aviation Authorities (CAA) are placing on Network Remote ID (Net-RID).

These Internet connected devices are herein called "Finders", as they find UAs by listening for B-RID messages. The Finders are B-RID forwarding proxies. Their potentially limited spacial view of RID messages could result in bad decisions on what messages to send to the SDSP and which to drop. Thus they will send all received messages and the SDSP will make any filtering decisions in what it forwards into the UAS Traffic Management (UTM).

Finders can be smartphones, tablets, connected cars, or any computing platform with Internet connectivity that can meet the requirements defined in this document. It is not expected, nor necessary, that Finders have any information about a UAS beyond the content in the B-RID messages.

Finders MAY only need a loose association with the SDSP(s). They may only have the SDSP’s Public Key and FQDN. It would use these, along with the Finder’s Public Key to use Elliptic Curve Integrated Encryption Scheme (ECIES), or other security methods, to send the messages in a secure manner to the SDSP. The SDSP MAY require a stronger relationship to the Finders. This may range from the Finder’s Public Key being registered to the SDSP with other information so that the SDSP has some level of trust in the Finders to requiring transmissions be sent over long-lived transport connections like ESP or DTLS.

If a 1-way only secure packet forwarding method is used (e.g., not a TCP connection), the Finder SHOULD receive periodic "heartbeats" from the SDSP to inform it that its transmissions are being received. The SDSP sets the rules on when to send these heartbeats as discuss below in Section 4.1.
1.1. Role of Supplemental Data Service Provider (SDSP)

The DRIP Architecture [I-D.ietf-drip-arch] introduces the basic CS-RID entities including CS-RID Finder and CS-RID SDSP. This document has minimal information about the actions of SDSPs. In general the SDSP is out of scope of this document. That said, the SDSPs should not simply proxy B-RID messages to the UTM(s). They should perform some minimal level of filtering and content checking before forwarding those messages that pass these tests in a secure manner to the UTM(s).

The SDSPs are also capable of maintaining a monitoring map, based on location of active Finders. UTMs may use this information to notify authorized observers of where there is and there is not monitoring coverage. They may also use this information of where to place proactive monitoring coverage.

An SDSP should only forward Authenticated B-RID messages like those defined in [drip-authentication] to the UTM(s). Further, the SDSP SHOULD validate the Remote ID (RID) and the Authentication signature before forwarding anything from the UA, and flagging those RIDs that were not validated. The SDSP MAY forward all B-RID messages to the UTM, leaving all decision making on B-RID messages veracity to the UTM.

When 3 or more Finders are reporting to an SDSP on a specific UA, the SDSP is in a unique position to perform multilateration on these messages and compute the Finder’s view of the UA location to compare with the UA Location/Vector messages. This check against the UA’s location claims is both a validation on the UA’s reliability as well as the trustworthiness of the Finders. Other than providing data to allow for multilateration, this SDSP feature is out of scope of this document. This function is limited by the location accuracy for both the Finders and UA.

1.2. Draft Status

This draft is still incomplete. New features are being added as capabilities are researched. The actual message formats also still need work.

2. Terms and Definitions
2.1. Requirements Terminology

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

This document uses terms defined in [RFC9153] and [I-D.ietf-drip-arch].

2.2. Definitions

B-RID: Broadcast Remote ID. A method of sending RID messages as 1-way transmissions from the UA to any Observers within radio range.

ECIES: Elliptic Curve Integrated Encryption Scheme. A hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks.

Finder: In Internet connected device that can receive B-RID messages and forward them to a UTM.

Multilateration: Multilateration (more completely, pseudo range multilateration) is a navigation and surveillance technique based on measurement of the times of arrival (TOAs) of energy waves (radio, acoustic, seismic, etc.) having a known propagation speed.

Net-RID: Network Remote ID. A method of sending RID messages via the Internet connection of the UAS directly to the UTM.

3. Problem Space

3.1. Meeting the needs of Network Remote ID

The USA Federal Aviation Authority (FAA), in the January 2021 Remote ID Final rule [FAA-FR], postponed Network Remote ID (Net-RID) and focused on Broadcast Remote ID. This was in response to the UAS vendors comments that Net-RID places considerable demands on then currently used UAS.

However, Net-RID, or equivalent, is necessary for UTM and knowing what soon may be in an airspace. A method that proxies B-RID into UTM can function as an interim approach to Net-RID and continue as a adjunct to Net-RID.
3.2. Advantages of Broadcast Remote ID

B-RID has its advantages over Net-RID.

* B-RID can more readily be implemented directly in the UA. Net-RID will more frequently be provided by the GCS or a pilot’s Internet connected device.
  - If Command and Control (C2) is bi-directional over a direct radio connection, B-RID could be a straightforward addition.
  - Small IoT devices can be mounted on UA to provide B-RID.
* B-RID can also be used by the UA to assist in Detect and Avoid (DAA).
* B-RID is available to observers even in situations with no Internet like natural disaster situations.

3.3. Trustworthiness of Proxied Data

When a proxy is introduced in any communication protocol, there is a risk of corrupted data and DOS attacks.

The Finders, in their role as proxies for B-RID, are authenticated to the SDSP (see Section 4). The SDSP can compare the information from multiple Finders to isolate a Finder sending fraudulent information. SDSPs can additionally verify authenticated messages that follow [drip-authentication].

The SPDP can manage the number of Finders in an area (see Section 4.3) to limit DOS attacks from a group of clustered Finders.

3.4. Defense against fraudulent RID Messages

The strongest defense against fraudulent RID messages is to focus on [drip-authentication] conforming messages. Unless this behavior is mandated, SPDPs will have to use assorted algorithms to isolate messages of questionable content.

4. The Finder – SDSP Security Relationship

The SDSP(s) and Finders SHOULD use EDDSA [RFC8032] keys as their trusted Identities. The public keys SHOULD be registered DRIP UAS Remote ID [I-D.ietf-drip-rid] and [I-D.ietf-drip-registries]. Other similar methods may be used.
During this registration, the Finder gets the SDSP’s EdDSA Public Key. These Public Keys allow for the following options for authenticated messaging from the Finder to the SDSP.

The SDSP uses some process (out of scope here) to register the Finders and their EDDSA Public Key. During this registration, the Finder gets the SDSP’s EDDSA Public Key. These Public Keys allow for the following options for authenticated messaging from the Finder to the SDSP.

1. ECIES can be used with a unique nonce to authenticate each message sent from a Finder to the SDSP.

2. ECIES can be used at the start of some period (e.g. day) to establish a shared secret that is then used to authenticate each message sent from a Finder to the SDSP sent during that period.

3. HIP [RFC7401] can be used to establish a session secret that is then used with ESP [RFC4303] to authenticate each message sent from a Finder to the SDSP.

4. DTLS [RFC5238] can be used to establish a secure connection that is then used to authenticate each message sent from a Finder to the SDSP.

4.1. SDSP Heartbeats

If a 1-way messaging approach is used (e.g. not TCP-based), the SDSP SHOULD send a heartbeat at some periodicity to the Finders so that they get confirmation that there is a receiver of their transmissions.

A simple (see Section 6.6) message that identifies the SDSP is sent to the Finder per some published policy of the SDSP. For example, at the first reception by the SDSP for the day, then the 1st for the hour. It is NOT recommended for the SDSP to send a heartbeat for every message received, as this is a potential DOS attack against the SDSP.

4.2. The Finder Map

The Finders are regularly providing their SDSP with their location. This is through the B-RID Proxy Messages and Finder Location Update Messages. With this information, the SDSP can maintain a monitoring map. That is a map of where there Finder coverage.
4.3. Managing Finders

Finder density will vary over time and space. For example, sidewalks outside an urban train station can be packed with pedestrians at rush hour, either coming or going to their commute trains. An SDSP may want to proactively limit the number of active Finders in such situations.

Using the Finder mapping feature, the SDSP can instruct Finders to NOT proxy B-RID messages. These Finders will continue to report their location and through that reporting, the SDSP can instruct them to again take on the proxying role. For example a Finder moving slowly along with dozens of other slow-moving Finders may be instructed to suspend proxying. Whereas a fast-moving Finder at the same location (perhaps a connected car or a pedestrian on a bus) would not be asked to suspend proxying as it will soon be out of the congested area.

5. UA location via multilateration

The SDSP can confirm/correct the UA location provided in the Location/Vector message by using multilateration on data provided by at least 3 Finders that reported a specific Location/Vector message (Note that 4 Finders are needed to get altitude sign correctly). In fact, the SDSP can calculate the UA location from 3 observations of any B-RID message. This is of particular value if the UA is only within reception range of the Finders for messages other than the Location/Vector message.

This feature is of particular value when the Finders are fixed assets around a high value site like an airport or large public venue.

5.1. GPS Inaccuracy

Single-band, consumer grade, GPS on small platforms is not accurate, particularly for altitude. Longitude/latitude measurements can easily be off by 3M based on satellite position and clock accuracy. Altitude accuracy is reported in product spec sheets and actual tests to be 3x less accurate. Altitude accuracy is hindered by ionosphere activity. In fact, there are studies of ionospheric events (e.g. 2015 St. Patrick's day [gps-ionosphere]) as measured by GPS devices at known locations. Thus where a UA reports it is rarely accurate, but may be accurate enough to map to visual sightings of single UA.

Smartphones and particular smartwatches are plagued with the same challenge, though some of these can combine other information like cell tower data to improve location accuracy. FCC E911 accuracy, by FCC rules is NOT available to non-E911 applications due to privacy.
concerns, but general higher accuracy is found on some smart devices than reported for consumer UA. The SDSP MAY have information on the Finder location accuracy that it can use in calculating the accuracy of a multilaterated location value. When the Finders are fixed assets, the SDSP may have very high trust in their location for trusting the multilateration calculation over the UA reported location.

6. The CS-RID Messages

The CS-RID messages between the Finders and the SDSPs primarily support the proxy role of the Finders in forwarding the B-RID messages. There are also Finder registration and status messages.

CS-RID information is represented in CBOR [RFC7049]. COSE [RFC8152] MAY be used for CS-RID MAC and COAP [RFC7252] for the CS-RID protocol. The CDDL [RFC8610] specification is used for CS-RID message description.

The following is a general representation of the content in the CS-RID messages.

```plaintext
(  
  CS-RID MESSAGE TYPE,
  CS-RID MESSAGE CONTENT,
  CS-RID MAC
)
```

The CS-RID MESSAGE CONTENT varies by MESSAGE TYPE.

6.1. CS-RID MESSAGE TYPE

The CS-RID MESSAGE TYPE is defined in Figure 1:

<table>
<thead>
<tr>
<th>Number</th>
<th>CS-RID Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
</tr>
<tr>
<td>1</td>
<td>B-RID Forwarding</td>
</tr>
<tr>
<td>2</td>
<td>Finder Registration</td>
</tr>
<tr>
<td>3</td>
<td>SDSP Response</td>
</tr>
<tr>
<td>4</td>
<td>Finder Location</td>
</tr>
<tr>
<td>5</td>
<td>SDSP Heartbeat</td>
</tr>
</tbody>
</table>

Figure 1
6.1.1. CDDL description for CS-RID message type

The overall CS-RID CDDL description is structured in Figure 2.

```
CSRID_Object = {
      application-context,
      info => info_message,
      proxy_message => broadcast_rid_proxy_message,
      finder_registration => finder_registration_message,
      sdsp_response => sdsp_response_message,
      location_update => location_update_message,
      sdsp_heartbeat => sdsp_heartbeat_message,
    }

info_message = {
      common_message_members,
      message_content => tstr,
    }

common_message_members = {
      message_type => message_types,
      mac_address => #6.37(bstr),
    }

message_types = &{
      Reserved : 0,
      BRD : 1,
      Finder-Registration : 2,
      SDSP-Response : 3,
      Finder-Location : 4,
    }
```

Figure 2

The application context rule is defined in Figure 3 for CS-RID application identification and version negotiation.

```
application-context = {
      application => "DRIP-CSRID",
      ? version => uint .size(1..2),
    }
```

Figure 3

The predefined CDDL text string labels (author note: for JSON currently, will move to CBOR uint keys in upcoming versions) used in the specification is listed in Figure 4.
6.2. The CS-RID B-RID Proxy Message

The Finders add their own information to the B-RID messages, permitting the SDSP(s) to gain additional knowledge about the UA(s). The RID information is the B-RID message content plus the MAC address. The MAC address is critical, as it is the only field that links a UA’s B-RID messages together. Only the ASTM Basic ID Message and possibly the Authentication Message contain the UAS ID field.

The Finders add an SDSP assigned ID, a 64 bit timestamp, GPS information, and type of B-RID media to the B-RID message. Both the timestamp and GPS information are for when the B-RID message(s) were received, not forwarded to the SDSP. All this content is MACed using a key shared between the Finder and SDSP.

The following is a representation of the content in the CS-RID messages.
(  
    CS-RID MESSAGE TYPE,  
    CS-RID ID,  
    RECEIVE TIMESTAMP,  
    RECEIVE GPS,  
    RECEIVE RADIO TYPE,  
    B-RID MAC ADDRESS,  
    B-RID MESSAGE,  
    CS-RID MAC  
)

6.2.1. CS-RID ID

The CS-RID ID is the ID recognized by the SDSP. This may be an HHIT [I-D.ietf-drip-rid], or any ID used by the SDSP.

6.2.2. CDDL description for CS-RID B-RID Proxy Message

The broadcast CS-RID proxy CDDL is defined in Figure 5

broadcast_rid_proxy_message = {  
    common_message_members,  
    rid => tstr,  
    timestamp => tdate,  
    gps => gps-coordinates,  
    radio_type => radio_types,  
    broadcast_mac_address => #6.37(bstr),  
    broadcast_message => #6.37(bstr),  
}

radio_types = &{  
    EFL : 0,  
    VLF : 1,  
    LF : 2,  
    MF : 3,  
    HF : 4,  
    HF : 5,  
    VHF : 6,  
    UHF : 7,  
    SHF : 8,  
    EHF : 9,  
}

gps-coordinates = [  
    latitude : float,  
    longitude : float,  
]
6.3. CS-RID Finder Registration

The CS-RID Finder MAY use [RFC7401] with the SDSP to establish a Security Association and a shared secret to use for the CS-RID MAC generation. In this approach, the HIP mobility functionality and [RFC4303] support are not used.

When HIP is used as above, the Finder Registration is a SDSP "wake up". It is sent prior to the Finder sending any proxied B-RID messages to ensure that the SDSP is able to receive and process the messages.

In this usage, the CS-RID ID is the Finder HIT. If the SDSP has lost state with the Finder, it initiates the HIP exchange with the Finder to reestablish HIP state and a new shared secret for the CS-RID B-RID Proxy Messages. In this case the Finder Registration Message is:

```
(  
  CS-RID MESSAGE TYPE,  
  CS-RID ID,  
  CS-RID TIMESTAMP,  
  CS-RID GPS,  
  CS-RID MAC  
)
```

6.3.1. CDDL description for Finder Registration

The CDDL for CS-RID Finder Registration is defined in Figure 6

```
finder_registration_message = {  
  common_message_members,  
  rid => tstr,  
  timestamp => tdate,  
  gps => gps-coordinates,  
}  

gps-coordinates = [  
  latitude : float,  
  longitude: float,  
]
```

Figure 6
6.4. CS-RID SDSP Response

The SDSP MAY respond to any Finder messages to instruct the Finder on its behavior.

\[
(\text{CS-RID MESSAGE TYPE, SDSP ID, CS-RID ID, CS-RID PROXY STATUS, CS-RID UPDATE INTERVAL, CS-RID MAC})
\]

The Proxy Status instructs the Finder if it should actively proxy B-RID messages, or suspend proxying and only report its location.

The Update Interval is the frequency that the Finder SHOULD notify the SDSP of its current location using the Location Update message.

6.4.1. CDDL description for SDSP Response

The CDDL for CS-RID SDSP response is defined in Figure 7

```cddl
sdsp_response_message = {
    common_message_members,
    sdsp_id => tstr,
    rid => tstr,
    proxy_status_type => proxy_status_types,
    update_interval => uint,
}

gps-coordinates = [
    latitude : float,
    longitude: float,
]

proxy_status_types = &(
    0: "forward",
    1: "reverse",
    2: "bi-directional",
)
```

Figure 7
6.5. CS-RID Location Update

The Finder SHOULD provide regular location updates to the SDSP. The interval is based on the Update Interval from Section 6.4 plus a random slew less than 1 second. The Location Update message is only sent when no other CS-RID messages, containing the Finder’s GPS location, have been sent since the Update Interval.

If the Finder has not received a SDSP Registration Response, a default of 5 minutes is used for the Update Interval.

(  
  CS-RID MESSAGE TYPE,  
  CS-RID ID,  
  CS-RID TIMESTAMP,  
  CS-RID GPS,  
  CS-RID MAC  
)

6.5.1. CDDL description for Location Update

The CDDL for CS-RID Location update is defined in Figure 8.

location_update_message = {  
  common_message_members,  
  rid => tstr,  
  timestamp => tdate,  
  gps => gps-coordinates,  
}

gps-coordinates = [  
  latitude : float,  
  longitude: float,  
]

Figure 8

6.6. SDSP Heartbeat

The SDSP SHOULD send a heartbeat message at some periodicity to the Finders so that they get confirmation that there is a receiver of their transmissions.

(  
  CS-RID MESSAGE TYPE,  
  SDSP ID,  
  CS-RID TIMESTAMP,  
)

Moskowitz, et al. Expires 11 November 2022
6.6.1. CDDL description for SDSP Heartbeat

The CDDL for CS-RID Heartbeat is defined in Figure 9.

sdsp_heartbeat_messagege = {
    common_message_members,
    sdsp_id  => tstr,
    timestamp => tdate,
}

Figure 9

7. The Full CS-RID CDDL specification

<CODE BEGINS>
; CDDL specification for Crowd source RID
; It specifies a collection of CS message types
;
;
; The CSRID overall data structure

CSRID_Object = {
    application-context,
    info => info_message,
    proxy_message => broadcast_rid_proxy_message,
    finder_registration => finder_registration_message,
    sdsp_response => sdsp_response_message,
    location_update => location_update_message,
}

; Application context: general information about CSRID message

application-context = {
    application => "DRIP-CSRID", ; TBD: consider CBOR tag
    ? version => uint .size(1..2),
}

; These members are include in every message
common_message_members = {
    message_type => message_types,
    mac_address => #6.37(bstr),
}

; CSRID message general information
info_message = {
    common_message_members,
    message_content => tstr,
}

broadcast_rid_proxy_message = {
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
    radio_type => radio_types,
    broadcast_mac_address => #6.37(bstr)
    broadcast_message => #6.37(bstr)
}

finder_registration_message = {
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
}

sdsp_response_message = {
    common_message_members,
    sdsp_id => tstr,
    rid => tstr,
    proxy_status_type => proxy_status_types,
    update_interval => uint,
}

location_update_message = {
    common_message_members,
    rid => tstr,
    timestamp => tdate,
    gps => gps-coordinates,
}

; ; Common rule definition

message_types = &{
    Reserved : 0,
    BRD : 1,
    Finder-Registration : 2,
    SDSP-Response : 3,
    Finder-Location : 4,
}
gps-coordinates = [  
    lat: float,  
    long: float,  
]

; Radio types, choose from one of radio_types (required)  
radio_types = &({  
    EFL : 0,  
    VLF : 1,  
    LF  : 2,  
    MF  : 3,  
    HF  : 4,  
    VHF : 6,  
    UHF : 7,  
    SHF : 8,  
    EHF : 9,  
})

proxy_status_types = &({  
    0: "forward",  
    1: "reverse",  
    2: "bi",  
})

; JSON label names

application = "application"  
version = "version"  
info = "message_info"  
proxy_message = "proxy_message-type"  
finder_registration = "finder_registration"  
sdsp_response = "sdsp_response"  
location_update = "location_update"  
rid = "id"  
message_type = "message_type"  
mac_address = "mac_address"  
message_content = "message_content"  
timestamp = "timestamp"  
gps = "gps"  
radio_type = "radio_type"  
broadcast_mac_address = "broadcast_mac_address"  
broadcast_message = "broadcast_message"  
sdsp_id = "sdsp_id"  
proxy_status_type = "proxy_status_type"  
update_interval = "update_interval"
8. IANA Considerations

TBD

9. Security Considerations

TBD

9.1. Privacy Concerns

TBD

10. References

10.1. Normative References


10.2. Informative References

[drip-authentication]
Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats & Protocols for Broadcast Remote


Appendix A. Using LIDAR for UA location

If the Finder has LIDAR or similar detection equipment (e.g. on a connected car) that has full sky coverage, the Finder can use this equipment to locate UAs in its airspace. The Finder would then be able to detect non-participating UAs. A non-participating UA is one that the Finder can "see" with the LIDAR, but not "hear" any B-RID messages.

These Finders would then take the LIDAR data, construct appropriate B-RID messages, and forward them to the SPDP as any real B-RID messages. There is an open issue as what to use for the actual RemoteID and MAC address.

The SDSP would do the work of linking information on a non-participating UA that it has received from multiple Finders with LIDAR detection. In doing so, it would have to select a RemoteID to use.

A seemingly non-participating UA may actually be a UA that is beyond range for its B-RID but in the LIDAR range.

This would provide valuable information to SDSPs to forward to UTMs on potential at-risk situations.
At this time, research on LIDAR and other detection technology is needed. There are full-sky LIDAR for automotive use with ranges varying from 20M to 250M. Would more than UA location information be available? What information can be sent in a CS-RID message for such "unmarked" UAs?

Acknowledgments

The Crowd Sourcing idea in this document came from the Apple "Find My Device" presentation at the International Association for Cryptographic Research’s Real World Crypto 2020 conference.

Authors’ Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

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

Shuai Zhao
Intel
2200 Mission College Blvd
Santa Clara, CA 95054
United States of America
Email: shuai.zhao@ieee.org
UAS Operator Privacy for RemoteID Messages
draft-moskowitz-drip-operator-privacy-10

Abstract

This document describes a method of providing privacy for UAS Operator/Pilot information specified in the ASTM UAS Remote ID and Tracking messages. This is achieved by encrypting, in place, those fields containing Operator sensitive data using a hybrid ECIES.

Status of This Memo

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

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

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

This Internet-Draft will expire on 10 October 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

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

This document defines a mechanism to provide privacy in the ASTM Remote ID and Tracking messages [F3411-19] by encrypting, in place, those fields that contain sensitive UAS Operator/Pilot information. Encrypting in place means that the ciphertext is exactly the same length as the cleartext, and directly replaces it.

An example of and an initial application of this mechanism is the 8 bytes of UAS Operator/Pilot (hereafter called simply Operator) longitude and latitude location in the ASTM System Message (Msg Type 0x4). This meets the Drip Requirements [RFC9153], Priv-01.

It is assumed that the Operator, via the UAS, registers an operation with its USS. During this operation registration, the UAS and USS exchange public keys to use in the hybrid ECIES. The USS key may be
long lived, but the UAS key SHOULD be unique to a specific operation. This provides protection if the ECIES secret is exposed from prior operations.

The actual Tracking message field encryption MUST be an "encrypt in place" cipher. There is rarely any room in the tracking messages for a cipher IV or encryption MAC (AEAD tag). There is rarely any data in the messages that can be used as an IV. The AES-CFB16 mode of operation proposed here can encrypt a multiple of 2 bytes.

The System Message is not a simple, one-time, encrypt the PII with the ECIES derived key. The Operator may move during a operation and these fields change, correspondingly. Further, not all messages will be received by the USS, so each message’s encryption must stand on its own and not be at risk of attack by the content of other messages.

Another candidate message is the optional ASTM Operator ID Message (Msg Type 0x5) with its 20 character Operator ID field. The Operator ID does not change during an operation, so this is a one-time encryption operation for the operation. The same cipher SHOULD be used for all messages from the UAS and this will influence the cipher selection.

Future applications of this mechanism may be provided. The content of the System Message may change to meet CAA requirements, requiring encrypting a different amount of data. At that time, they will be added to this document.

Editor note: The Rules for allowing encryption need to be updated to handle the UA operating in Broadcast Remote ID only mode. That is conditions where the USS cannot notify the UAS to stop encrypting.

2. Terms and Definitions

2.1. Requirements Terminology

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

2.2. Definitions

See Section 2.2 of [RFC9153] for common DRIP terms.
ECIES
Elliptic Curve Integrated Encryption Scheme. A hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks.

Keccak (KECCAK Message Authentication Code):
The family of all sponge functions with a KECCAK-f permutation as the underlying function and multi-rate padding as the padding rule. It refers in particular to all the functions referenced from [NIST.FIPS.202] and [NIST.SP.800-185].

KMAC (KECCAK Message Authentication Code):
A PRF and keyed hash function based on KECCAK.

3. The Operator - USS Security Relationship

All CAAs have rules defining which UAS must be registered to operate in their National Airspace. This includes UAS and Operator registration in a USS. Further, operator’s are expected to report flight operations to their USS. This operation reporting provides a mechanism for the USS and operator to establish an operation security context. Here it will be used to exchange public keys for use in ECIES.

The operator’s ECIES public key SHOULD be unique for each operation. The USS ECIES public key may be unique for each operator and operation, but not required. For best post-compromise security (PCS), the USS ECIES public key should be changed over some operational window.

The public key algorithm should be Curve25519 [RFC7748]. Correspondingly, the ECIES 128 bit shared secret should be generated using KMAC [NIST.SP.800-185].

3.1. ECIES Shared Secret Generation

The KMAC function provides a new, more efficient, key derivation function over HKDF [RFC5869]. This will be referred to as KKDF.

HKDF needs a minimum of 4 hash functions (e.g. SHA256). KKDF does an equivalent shared secret generation in a single Keccak Sponge operation.

When the USS - UAS Operation Security Context is established, the UAS provides its UAS ID (null padded to 20 characters per [F3411-19]) and a 256 bit random nonce to the USS. These are inputs, along with the ECDH keys to produce the shared secret as follows.
A 64 bit UNIX timestamp for the operation time is also included in the Operation Security Context. This will be used in the IV construction.

Per [NIST.SP.800-56Cr1], Section 4.1, Option 3:

\[ \text{Shared Secret} = \text{KMAC128}(\text{salt}, \text{IKM}, L, S) \]

L is the derived key bit length. Since only a single key is needed, \( L=128 \).

S is the byte string 01001011 || 01000100 || 01000110, which represents the sequence of characters "K", "D", and "F" in 8-bit ASCII.

\[ \text{salt} = \text{Nonce-USS} \mid \text{Nonce-UAS} \]

There are special security considerations for IKM per [RFC7748]. The IKM as follows:

\[ \text{IKM} = \text{Diffie-Hellman secret} \mid \text{USS-ID} \mid \text{RID} \]

4. System Message Privacy

The System Message contains 8 bytes of Operator specific information: Longitude and Latitude of the Remote Operator (Pilot in the field description) of the UA. The GCS MAY encrypt these as follows.

Editors Note: The next version of [F3411-19], currently in ballot, is adding a 2 byte Operator Altitude field, thus increasing the Operator specific information to 10 bytes. This change will be delineated via Protocol Version field. It is this future shift from a multiple of 4 bytes to a multiple of 2 bytes that is the reason to change from CFB32 in earlier drafts to CFB16 used now.

The 8 bytes of Operator information are encrypted, using the ECIES derived 128 bit shared secret, with one of the cipher’s specified below. The choice of cipher is based on USS policy and is agreed to as part of the operation registration. AES-CFB16 is the recommended default cipher.

ASTM Remote ID and Tracking messages [F3411-19] SHOULD be updated to allow Bit 5 of the Flags byte in the System Message set to "1" to indicate the Operator information is encrypted.

The USS similarly decrypts these 8 bytes and provides the information to authorized entities.
4.1. Rules for encrypting System Message content

If the Operator location is encrypted the encrypted bit flag MUST be set to 1.

The Operator MAY be notified by the USS that the operation has entered a location or time where privacy of Operator location is not allowed. In this case the Operator MUST disable this privacy feature and send the location unencrypted or land the UA or route around the restricted area.

If the UAS loses connectivity to the USS, the privacy feature SHOULD be disabled or land the UA.

If the operation is in an area or time with no Internet Connectivity, the privacy feature MUST NOT be used.

4.2. Rules for decrypting System Message content

An Observer receives a System Message with the encrypt bit set to 1. The Observer sends a query to its USS Display Provider containing the UA’s ID and the encrypted fields.

The USS Display Provider MAY deny the request if the Observer does not have the proper authorization.

The USS Display Provider MAY reply to the request with the decrypted fields if the Observer has the proper authorization.

The USS Display Provider MAY reply to the request with the decrypting key if the Observer has the proper authorization.

The Observer MAY notify the USS through its USS Display Provider that content privacy for a UAS in this location/time is not allowed. If the Observer has the proper authorization for this action, the USS notifies the Operator to disable this privacy feature.

5. Operator ID Message Privacy

The Operator ID Message contains the 20 byte Operator ID. The GCS MAY encrypt these as follows.

The 20 bytes Operator ID is encrypted, using the ECIES derived 128 bit shared secret, with one of the cipher’s specified below. The choice of cipher is based on USS policy and is agreed to as part of the operation registration. AES-CFB16 is the recommended default cipher.
ASTM Remote ID and Tracking messages [F3411-19] SHOULD be updated to allow Operator ID Type in the Operator ID Message set to "1" to indicate the Operator ID is encrypted.

The USS similarly decrypts these 20 bytes and provides the information to authorized entities.

5.1. Rules for encrypting Operator ID Message content

If the Operator ID is encrypted the Operator ID Type field MUST be set to 1.

The Operator MAY be notified by the USS that the operation has entered a location or time where privacy of Operator ID is not allowed. In this case the Operator MUST disable this privacy feature and send the ID unencrypted or land the UA or route around the restricted area.

If the UAS loses connectivity to the USS, the privacy feature SHOULD be disabled or land the UA.

If the operation is in an area or time with no Internet Connectivity, the privacy feature MUST NOT be used.

5.2. Rules for decrypting Operator ID Message content

An Observer receives a Operator ID Message with the Operator ID Type field set to 1. The Observer sends a query to its USS Display Provider containing the UA’s ID and the encrypted fields.

The USS Display Provider MAY deny the request if the Observer does not have the proper authorization.

The USS Display Provider MAY reply to the request with the decrypted fields if the Observer has the proper authorization.

The USS Display Provider MAY reply to the request with the decrypting key if the Observer has the proper authorization.

The Observer MAY notify the USS through its USS Display Provider that content privacy for a UAS in this location/time is not allowed. If the Observer has the proper authorization for this action, the USS notifies the Operator to disable this privacy feature.

6. Cipher choices for Operator PII encryption
6.1. Using AES-CFB16

CFB16 is defined in [NIST.SP.800-38A], Section 6.3. This is the Cipher Feedback (CFB) mode operating on 16 bits at a time. This variant of CFB can be used to encrypt any multiple of 2 bytes of cleartext.

The Operator includes a 64 bit UNIX timestamp for the operation time, along with its operation public key. The Operator also includes the UA MAC address (or multiple addresses if flying multiple UA).

The 128 bit IV for AES-CFB16 is constructed by the Operator and USS as: SHAKE128(MAC||UTCTime||Message_Type, 128). Inclusion of the ASTM Message_Type ensures a unique IV for each Message type that contains PII to encrypt.

AES-CFB16 would then be used to encrypt the Operator information.

6.2. Using a Feistel scheme

If the encryption speed doesn’t matter, we can use the following approach based on the Feistel scheme. This approach is already being used in format-preserving encryption (e.g. credit card numbers). The Feistal scheme is explained in Appendix A.

6.3. Using AES-CTR

If 2 bytes of the Message can be set aside to contain a counter that is incremented each time the Operator information changes, AES-CTR can be used as follows.

The Operator includes a 64 bit UNIX timestamp for the operation time, along with its operation public key. The Operator also includes the UA MAC address (or multiple addresses if flying multiple UA).

The high order bits of an AES-CTR counter is constructed by the Operator and USS as: SHAKE128(MAC||UTCTime||Message_Type, 112). Inclusion of the ASTM Message_Type ensures a unique IV for each Message type that contains PII to encrypt.

AES-CTR would then be used to encrypt the Operator information.

7. DRIP Requirements addressed

This document provides solution to PRIV-1 for PII in the ASTM System Message.
8. ASTM Considerations

ASTM will need to make the following changes to the "Flags" in the System Message (Msg Type 0x4):

Bit 5:
  Value 1 for encrypted; 0 for cleartext (see Section 4).

ASTM will need to make the following changes to the "Operator ID Type" in the Operator ID Message (Msg Type 0x5):

Operator ID Type
  Value 1 for encrypted Operator ID (see Section 5).

9. IANA Considerations

TBD

10. Security Considerations

An attacker has no known text after decrypting to determine a successful attack. An attacker can make assumptions about the high order byte values for Operator Longitude and Latitude that may substitute for known cleartext. There is no knowledge of where the operator is in relation to the UA. Only if changing location values "make sense" might an attacker assume to have revealed the operator’s location.

10.1. CFB16 Risks

Using the same IV for different Operator information values with CFB16 presents a cryptoanalysis risk. Typically only the low order bits would change as the Operators position changes. The risk is mitigated due to the short-term value of the data. Further analysis is need to properly place risk.

10.2. Crypto Agility

The ASTM Remote ID Messages do not provide any space for a crypto suite indicator or any other method to manage crypto agility.

All crypto agility is left to the USS policy and the relation between the USS and operator/UAS. The selection of the ECIES public key algorithm, the shared secret key derivation function, and the actual symmetric cipher used for on the System Message are set by the USS which informs the operator what to do.
10.3. Key Derivation vulnerabilities

[RFC7748] warns about using Curve25519 and Curve448 in Diffie-Hellman for key derivation:

Designers using these curves should be aware that for each public key, there are several publicly computable public keys that are equivalent to it, i.e., they produce the same shared secrets. Thus using a public key as an identifier and knowledge of a shared secret as proof of ownership (without including the public keys in the key derivation) might lead to subtle vulnerabilities.

This applies here, but may have broader consequences. Thus two endpoint IDs are included with the Diffie-Hellman secret.

10.4. KMAC Security as a KDF

Section 4.1 of NIST SP 800-185 [NIST.SP.800-185] states:

"The KECCAK Message Authentication Code (KMAC) algorithm is a PRF and keyed hash function based on KECCAK. It provides variable-length output."

That is, the output of KMAC is indistinguishable from a random string, regardless of the length of the output. As such, the output of KMAC can be divided into multiple substrings, each with the strength of the function (KMAC128 or KMAC256) and provided that a long enough key is used, as discussed in Sec. 8.4.1 of SP 800-185.

For example KMAC128(K, X, 512, S), where K is at least 128 bits, can produce 4 128 bit keys each with a strength of 128 bits. That is a single sponge operation is replacing perhaps 5 HMAC-SHA256 operations (each 2 SHA256 operations) in HKDF.

11. Normative References

[NIST.FIPS.202]
[NIST.SP.800-185]  

[NIST.SP.800-38A]  

[NIST.SP.800-56C1]  

[RFC2119]  

[RFC8174]  

12. Informative References

[F3411-19]  

[RFC5869]  

[RFC7748]  
Appendix A. Feistel Scheme

This approach is already being used in format-preserving encryption.

According to the theory, to provide CCA security guarantees (CCA = Chosen Ciphertext Attacks) for m-bit encryption X \(\rightarrow\) Y, we should choose \(d \geq 6\). It seems very ineffective that when shortening the block length, we have to use 6 times more block encryptions. On the other hand, we preserve both the block cipher interface and security guarantees in a simple way.

How to encrypt an m-bit plaintext X using an n-bit block cipher \(E = \{E_K\}\) for \(n > m\)?

\[
\text{Enc}(X, K):
\begin{align*}
1. & \ Y \leftarrow X. \\
2. & \text{Split } Y \text{ into 2 equal parts: } Y = Y_1 || Y_2 \\
& (\text{let us assume for simplicity that } m \text{ is even}). \\
3. & \text{For } i = 1, 2, \ldots, d \text{ do:} \\
& \quad Y \leftarrow Y_2 || (Y_1 ^ \text{first}_m/2_\text{bits}(E_K(Y_2 || C_i)), \\
& \quad \text{where } C_i \text{ is a } (n - m/2)-\text{bit round constant}. \\
4. & \ Y \leftarrow Y_2 || Y_1. \\
5. & \text{Return } Y.
\end{align*}
\]

\[
\text{Dec}(Y, K):
\begin{align*}
1. & \ X \leftarrow Y. \\
2. & \text{Split } X \text{ into 2 equal parts: } X = X_1 || X_2. \\
3. & \text{For } i = d, \ldots, 2, 1 \text{ do:} \\
& \quad X \leftarrow X_2 || (X_1 ^ \text{first}_m/2_\text{bits}(E_K(X_2 || C_i)). \\
4. & \ X \leftarrow X_2 || X_1. \\
5. & \text{Return } X.
\end{align*}
\]

Acknowledgments

The recommended ciphers come from discussions on the IRTF CFRG mailing list.

Authors’ Addresses
Robert Moskowitz  
HTT Consulting  
Oak Park, MI 48237  
United States of America  
Email: rgm@labs.htt-consult.com

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
Secure UAS Network RID and C2 Transport
draft-moskowitz-drip-secure-nrid-c2-08

Abstract

This document defines a transport mechanism for Unmanned Aircraft System (UAS) Network Remote ID (Net-RID). The Broadcast Remote ID (B-RID) messages can be sent directly over UDP or via a more functional protocol using CoAP/CBOR for the Net-RID messaging. This is secured via either HIP/ESP or DTLS. HIP/ESP or DTLS secure messaging Command-and-Control (C2) for is also described.

Status of This Memo

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

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

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

This Internet-Draft will expire on 28 November 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights
1. Introduction

This document defines a set of messages for Unmanned Aircraft System (UAS) Network Remote ID (Net-RID) derived from the ASTM Remote ID [F3411-19] broadcast messages and common data dictionary. These messages are transported from the UAS to its USS Network Service Provider (Net-RID SP) either directly over UDP or via CoAP/CBOR ([RFC7252]/[RFC8949]).
Direct UDP, referred here as Minimal Net-RID (MNet-RID), and CoAP/CBOR were selected for their low communication "cost". This may not be an issue if Net-RID originates from the Ground Control Station (GCS, Section 3.1.2), but it may be an important determinant when originating from the UA (Section 3.1.1). Particularly, very small messages may open Net-RID transmissions over a variety of wireless technologies.

This document also defines mechanisms to provide secure transport for these Net-RID messages and Command and Control (C2) messaging.

A secure end-to-end transport for Net-RID (UAS to Network RID Service Provider (Net-RID SP)) also should provide full Confidentiality, Integrity, and Authenticity (CIA). It may seem that confidentiality is optional, as most of the information in Net-RID is sent in the clear in Broadcast Remote ID (B-RID), but this is a potentially flawed analysis. Net-RID has eavesdropping risks not in B-RID and may contain more sensitive information than B-RID. The secure transport for Net-RID should also manage IP address changes (IP mobility) for the UAS.

A secure end-to-end transport for C2 is critical for UAS especially for Beyond Line of Sight (BLOS) operations. It needs to provide data CIA. Depending on the underlying network technology, this secure transport may need to manage IP address changes (IP mobility) for both the UA and GCS.

Two options for secure transport are provided: HIP [RFC7401] with ESP [RFC7402] and DTLS 1.3 [DTLS-1.3-draft]. These options are generally defined and their applicability is compared and contrasted. It is up to Net-RID and C2 to select which is preferred for their situation.

MOBIKE [RFC5266] is an alternative to HIP for ESP key establishment. It functions enough like HIP that it was left out, but implied, for document simplicity. There may be some identity pieces needed to map HHITs and HIs to what MOBIKE uses.

To further reduce the communication cost, SCHC [RFC8724] is defined for both the direct UDP and CoAP layer [RFC8824]. For ESP "compression", ESP Implicit IV, [RFC8750] and Diet ESP [diet-esp] may be used together. SCHC for the IP/UDP layer is currently defined by IP carrier (e.g. LoRaWAN, [RFC9011]) and will be covered in any specific implementation.

2. Terms and Definitions
2.1. Requirements Terminology

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

2.2. Definitions

See Section 2.2 of [RFC9153] for common DRIP terms. The following new terms are used in this document:

**B-RID**
Broadcast Remote ID. A method of sending RID messages as 1-way transmissions from the UA to any Observers within radio range.

**MNet-RID**
A Minimal implementation of Network Remote ID, based on B-RID messages directly over UDP.

**Net-RID**
Network Remote ID. A method of sending RID messages via the Internet connection of the UAS directly to the UTM.

**RID**
Remote ID. A unique identifier found on all UA to be used in communication and in regulation of UA operation.

3. Network Remote ID

In UAS Traffic Management (UTM), the purpose of Net-RID is to provide situational awareness of UA (in the form of flight tracking) in a user specified 3D volume. The data needed for this is already defined in [F3411-19], but a standard message format, protocol, and secure communications methodology are missing. F3411, and other UTM based standards going through ASTM and other SDOs, provide JSON objects and some of the messages for passing information between various UTM entities (e.g., Net-RID SP to Net-RID SP and Net-RID SP to Net-RID DP) but does not specify how the data gets into UTM to begin with. This document will provide such an open standard.

A full-function CoAP-based Net-RID protocol is defined in Section 3.4. This provides for either transport of the appropriate B-RID messages and/or the [F3411-19] data elements encoded in CBOR.
A minimal messaging approach (MNet-RID, Section 3.3), only using the Broadcast Remote ID (B-RID) messages in [F3411-19], is sufficient to meet the needs of Net-RID. These messages can be sent to the Net-RID SP when their contents change. Further, a UAS supporting B-RID will have minimal development to add Net-RID support.

This approach has the added advantage of being very compact, minimizing the Net-RID communications cost.

Other messages may be needed in some Net-RID situations. Thus a simple message multiplexer is provided for MNet-RID and CoAP is defined for a richer messaging environment.

3.1. Network RID Endpoints

The US FAA defines the Network Remote ID endpoints as a USS Network Service Provider (Net-RID SP) and the UAS. Both of these are rather nebulous items and what they actually are will impact how communications flow between them.

The Net-RID SP may be provided by the same entity serving as the UAS Service Provider (USS). This simplifies a number of aspects of the Net-RID communication flow. The Net-RID SP is likely to be stable in the network, that is its IP address will not change during a mission. This simplifies maintaining the Net-RID communications.

The UAS component in Net-RID may be either the UA, GCS, or the Operator’s Internet connected device (e.g. smartphone or tablet that is not the GCS). In all cases, mobility MUST be assumed. That is the IP address of this end of the Net-RID communication may change during an operation. The Net-RID mechanism MUST support this. The UAS Identity for the secure connection may vary based on the UAS endpoint.

3.1.1. Net-RID from the UA

Some UA will be equipped with direct Internet access. These UA will also tend to have multiple radios for their Internet access (e.g., Cellular and WiFi). Thus multi-homing with "make before break" behavior is needed. This is on top of any IP address changes on any of the interfaces while in use.

Multicast (GEN-10 in [RFC9153]) over multiple Internet connection technologies MAY be used improve QOS (GEN-7 in [RFC9153]) for Net-RID. (Author’s question: Is this really qualify as multicast?)
3.1.2. Net-RID from the GCS

Many UA will lack direct Internet access, but their GCS are connected. As an Operator is expected to register an operation with its USS, this may be done via the Internet connected GCS. The GCS could then be the source of the secure connection for Net-RID (acting as a gateway).

There are two sources of the RID messages for the GCS, both from the UA. These are UA B-RID messages, or content from C2 messages that the GCS converts to RID message format. In either case, the GCS may be mobile with changing IP addresses. The GCS may be in a fast moving ground device (e.g. delivery van), so it can have as mobility demanding connection needs as the UA.

In a constrained wireless environment for the UA that is not functioning autonomously (i.e., at least C2 traffic to the GCS), this approach may be the most economical. It only uses the wireless to send the UA status once, to the GCS, that then provides the Net-RID functionality.

3.1.3. Net-RID from the Operator

Many UAS will have no Internet connectivity, but the UA is sending B-RID messages and the Operator, when within RF range, can receive these B-RID messages on an Internet Connected device that can act as the proxy for these messages, turning them into Net-RID messages.

3.2. Network RID Messaging

Net-RID messaging is tied to a UA operation (generally called a flight or mission). This consists of an initial secure link setup, followed by a set of mostly static information related to the operation. During the operation, continuous location information is sent by the UA with any needed updates to the mostly static operation information.

The Net-RID SP SHOULD send regular "heartbeats" to the UAS. If the UAS does not receive these heartbeats for some policy set time, the UA MUST take the policy set response to loss of Net-RID SP connectivity. For example, this could be a mandated immediate landing. There may be other messages from the Net-RID SP to the UAS (e.g., call the USS operator at this number NOW!). The UAS MUST follow acknowledge policy for these messages.

If the Net-RID SP stops receiving messages from the UAS (Section 3.2.3), it should notify the UTM of a non-communicating UA while still in operation.

3.2.1. Secure Link Setup

The secure link setup MUST be done before the operation begins, thus it can use a high capacity connection like WiFi. It MAY use the UA RID for this setup, including other data elements provided in the B-RID Basic ID (Msg Type 0x0) Message. If the Basic ID information is NOT included via the secure setup (including the Net-RID SP querying the USS for this information), it MUST be sent as part of the Static Messages (Section 3.2.2).

3.2.1.1. UAS Identity

The UAS MAY use its RID if it is a HHIT (DET per [drip-uas-rid]). It may use some other Identity, based on the Net-RID SP policy.

The GCS or Operator smart device may have a copy of the UA credentials and use them in the connection to the Net-RID SP. In this case, they are indistinguishable from the UA as seen from the Net-RID SP. Alternatively, they may use their own credentials with the Net-RID SP which would need some internal mechanism to tie that to the UA.

3.2.1.2. HIP for ESP Secure Link

HIP [RFC7401] for ESP Secure Link is a natural choice for a DET RID. For this, the Net-RID SP would also need a HHIT, possibly following the process in [drip-registries].

3.2.1.3. DTLS Secure Link

For DTLS [DTLS-1.3-draft] secure link, DANCE [dane-clients] may be used with a DET’s DNS lookup to retrieve a TLSA RR with the DET’s HI encoded in PKIX SubjectPublicKeyInfo format (per [RFC7250]).

The Net-RID SP DTLS credential may follow DANE [RFC6698] or any other DTLS server credential method.

3.2.2. Static Messages

For simplicity, a class of UAS information is called here “Static”, though in practice any of it can change during the operation, but will change infrequently. This information is the contents of the B-RID Self-ID (Msg Type 0x3), Operator ID (Msg Type 0x5), and System Messages (Msg Type 0x4). This information can simply be sent in the same format as the B-RID messages. Alternatively the individual data elements may be sent as separate CBOR objects.
The Basic ID (Msg Type 0x0) Message may be included as a static message if this information was not used for the secure setup. There may be more than one Basic ID Message needed if as in the case where the Japan Civil Aviation Bureau (JCAB) has mandated that the Civil Aviation Authority (CAA) assigned ID (UA ID type 2) and Serial Number (UA ID type 1) be broadcasted.

The information in the System Message is most likely to change during an operation. Notably the Operator Location data elements are subject to change if the GCS is physically moving (e.g., hand-held and the operator is walking or driving in a car). The whole System Message may be sent, or only the changing data elements as CBOR objects.

These static message elements may be sent before the operation begins, thus their transmission can use a high capacity connection like WiFi. Once the operation is underway, any updates will have to traverse the operational link which may be very constrained and this will impact data element formatting.

The Net-RID SP MUST acknowledge these messages. The UAS MUST receive these ACKs. If no ACK is received, the UAS MUST resend the message(s). This send/ACK sequence continues either until ACK is received, or some policy number of tries. If this fails, the UAS MUST act that the Net-RID SP connection is lost and MUST take the policy set response to loss of Net-RID SP connectivity. If the information changes during this cycle, the latest information MUST always be sent.

3.2.3. Vector/Location Message

Many CAAs mandate that the UA Vector/Location information be updated at least once per second. Without careful message design, this messaging volume would overwhelm many wireless technologies. Thus to enable the widest deployment choices, a highly compressed format is recommended.

The B-RID Vector/Location Message (Msg Type 0x1) is the simplest small object (24 bytes) for sending this information as a single CBOR object or via MNet-RID. It may be possible to send only those data elements that changed in the last time interval. This may result in smaller individual transmissions, but should not be used if the resulting message is larger than the Vector/Location Message.
3.3. The Minimal, UDP, Net-RID Protocol

The Minimal Network Remote ID protocol is a simple UDP messaging consisting of a 1-byte message type field and a message field of maximum 25-bytes length.

The Message Type Field is defined as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>RESERVED</td>
</tr>
<tr>
<td>1</td>
<td>B-RID Message</td>
</tr>
<tr>
<td>2</td>
<td>Net-RID SP ACK</td>
</tr>
<tr>
<td>3</td>
<td>Net-RID SP Heartbeat</td>
</tr>
</tbody>
</table>

The B-RID Message is 25 bytes:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B-RID Message Type/version</td>
</tr>
<tr>
<td>24</td>
<td>B-RID Message</td>
</tr>
</tbody>
</table>

The Net-RID SP ACK is 5 bytes:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Timestamp</td>
</tr>
<tr>
<td>1</td>
<td>B-RID Message Type/version from message ACKed</td>
</tr>
</tbody>
</table>

Should a 12byte hash of message be included as in Manifest?

The Net-RID SP Heartbeat is 4 bytes:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Timestamp</td>
</tr>
</tbody>
</table>

3.3.1. Compressing the MNet-RID message headers

The security envelope (ESP of DTLS) and UDP headers may be compressed to further minimize the communication cost of MN-RID.

3.3.1.1. Compressing ESP/UDP headers

A normal ESP/AES-GCM-12/UDP wrapper for the MNet-RID messages is 10+28+8=46 bytes. By applying the SCHC compression via [diet-esp] and using [RFC8750] Implicit Cipher IVs, this is reduced to 4+12+0=16 bytes.
AES-CCM-12 has a smaller, but valuable, size reduction on compression, as CCM’s IV is only 8 bytes compared to GCM’s 16-byte IV. Thus uncompressed, the wrapper is 10+20+8=38 bytes. Compressed it is 4+12+0=16 bytes. Or "over the wire", compressed CCM offers no improvements to GCM and its 2-pass process will tend to result in a poorer performance compared to GCM, even on these small messages. Thus GCM is the recommended mode-of-operation for AES.

Note that [RFC8750] does not provide implicit IV use for AES-GCM-12. At the time of writing the use case for the smaller ICV was not apparent. Here, the smaller hash is not a lower risk given the limited traffic within a single operation. If not provided elsewhere, this document will request ENCR_AES_GCM_12_IIV for IKE and both AES_GCM_12 and AES_GCM_12_IIV for HIP.

[diet-esp] may be completely statically configured, or may have HIP or IKE negotiated values. This will be determined by Net-RID SP policy.

TBD: diet-esp context and rules.

3.3.1.2. Compressing UDP/DTLS message headers

TBD. No current SCHC guidance for DTLS.

3.4. CoAP Net-RID messages

The CoAP based Net-RID protocol is intended for a richer conversation between the UAS and USS. The USS, through the Net-RID SP, may compare actual UA progress against the filed flight plan and against other UA actual traffic. The USS may then send to the UAS recommended changes to the flight plan to de-conflict traffic or advise the UAS to avoid hazards (1st responder event, avoid space). The UAS may then negotiate changes to the plan, and act on them, as appropriate.

This sort of advanced UAS behavior is envisioned as part of total UTM activities. Discussions now ongoing in UTM will provide the data models and transactional UAS/USS interactions, that will drive UAS communications past the MN-RID defined in Section 3.3 toward this more functional CoAP Net-RID protocol.
4. Command and Control

The Command and Control (C2) connection is between the UA and GCS. This is often over a direct link radio. Some times, particularly for BLOS, it is via Internet connections. In either case C2 SHOULD be secure from eavesdropping and tampering. For design and implementation consistency it is best to treat the direct link as a local link Internet connection and use constrained networking compression standards.

Both the UA and GCS need to be treated as fully mobile in the IP networking sense. Either one can have its IP address change and both could change at the same time (the double jump problem). It is preferable to use a peer-to-peer (P2P) secure technology like HIPv2 [RFC7401].

Finally UA may also tend to have multiple radios for their C2 communications. Thus multi-homing with "make before break" behavior is needed. This is on top of any IP address changes on any of the interfaces while in use.

4.1. Securing MAVLink

MAVLink [MAVLINK] is a commonly used protocol for C2 that uses UDP port 14550 for transport over IP. Message authenticity was added in MAVLink 2 in the form of a SHA-256 (secret | message) left-truncated to 6 byte. This does not follow HMAC [RFC2104] security recommendations, nor provides confidentiality.

The MAVlink authentication only provides 24-bit collision resistance but is not susceptible to a hash length attack. By following the security approach here, UAS C2 is superior to that currently provided within MAVlink. It provides 48-bit collision resistance and full confidentiality.

4.1.1. Compressed ESP for MAVlink

The approach in Section 3.3.1.1 can be used to fully secure MAVlink and include the UDP header for IP transport. Further, MAVlink itself can be compressed.

MAVlink messages contain a 1-byte Seq number and 2-byte CRC. Both of these can be generated from SCHC rules. These 3 bytes along with the 13-byte MAVlink signature provides the 16 bytes so that the over-the-wire cost is the same.
This secure MAVlink format may be sent directly over a local wireless link. The UDP port processing adds little cost. Sending this over IP provides the needed confidentiality at 8 bytes less than unencrypted messages.

TBD: MAVlink SCHC context and rules. These will be part of the MAVlink ESP setup.

4.2. Compressed UDP/DTLS for MAVlink

At this time, DTLS is NOT recommended for C2 security, as it is challenged with server mobility. It may be added at a later time.

5. Secure Transports

Secure UDP-based protocols are preferred for both Network Remote ID (Net-RID) and C2. Both HIPv2 and DTLS can be used. It will be shown below that HIPv2 is better suited in most cases.

For IPv6 and CoAP over both WiFi and Bluetooth (or any other radio link), SCHC [RFC8724] is defined to significantly reduce the per packet transmission cost. SCHC is used both within the secure envelope and before the secure envelope as shown in Section 5.2.10 of [lpwan-architecture]. For Bluetooth, there is also IPv6 over Bluetooth LE [RFC7668] for more guidance.

Local link (direct radio) C2 security is possible with the link’s MAC layer security. SCHC SHOULD still be used as above. Both WiFi and Bluetooth link security can provide appropriate security, but this would not provide trustworthy multi-homed security.

5.1. HIP for Secure Transport

HIP has already been used for C2 mobility, managing the ongoing connectivity over WiFi at start of an operation, switching to LTE once out of WiFi range, and returning to WiFi connectivity at the end of the operation. This functionality is especially important for BLOS. HHITs are already defined for RID, and need only be added to the GCS via a GCS Registration as part of the UAS to USS registration to be used for C2 HIP.

When the UA is the UAS endpoint for Net-RID (Section 3.1.1), and particularly when HIP is used for C2, HIP for Net-RID simplifies protocol use on the UA. The Net-RID SP endpoint may already support HIP if it is also the HHIT Registrar. If the UA lacks any IP ability and the RID HHIT registration was done via the GCS or Operator device, then they may also be set for using HIP for Net-RID.
Further, double jump and multi-homing support is mandatory for C2 mobility. This is inherent in the HIP design. The HIP address update can be improved with [hip-fast-mobility].

5.2. DTLS for Secure Transport

DTLS is a good fit for Net-RID for any of the possible UAS endpoints. There are challenges in using it for C2. To use DTLS for C2, the GCS will need to be the DTLS server. How does it 'push' commands to the UA? How does it reestablish DTLS security if state is lost? And finally, how is the double jump scenario handled?

All the above DTLS for C2 probably have solutions. None of them are inherent in the DTLS design.

5.3. Ciphers for Secure Transport

The cipher choice for either HIP or DTLS depends, in large measure, on the UAS endpoint. If the endpoint is computationallly constrained, the cipher computations become important. If any of the links are constrained or expensive, then the over-the-wire cost needs to be minimized. AES-CCM and AES-GCM are the preferred, modern, AEAD ciphers. Section 3.3.1.1 shows that proper compression can provide the more efficient GCM at no over-the-wire cost. Thus AES-GCM is the recommended AES mode-of-operation.

NIST is working on selecting a new lightweight cipher that may be the best choice for use on a UA. The Keccak Xoodyak cipher in [new-hip-crypto] is a good "Green Cipher".

5.4. HIP and DTLS contrasted and compared

This document specifies the use of DTLS 1.3 for its 0-RTT mobility feature and improved (over 1.2) handshake. DTLS 1.3 is still an IETF draft, so there is little data available to properly contrast it with HIPv2. This section will be based on the current DTLS 1.2. The basic client-server model is unchanged.

The use of DTLS vs HIPv2 (both over UDP, HIP in IPsec ESP BEET mode) has pros and cons. DTLS is currently at version 1.2 and based on TLS 1.2. It is a more common protocol than HIP, with many different implementations available for various platforms and languages.

DTLS implements a client-server model, where the client initiates the communication. In HIP, two parties are equal and either can be an Initiator or Responder of the Base Exchange. HIP provides separation between key management (base exchange) and secure transport (for example IPsec ESP BEET) while both parts are tightly coupled in DTLS.
DTLS 1.2 still has quite chatty connection establishment taking 3-5 RTTs and 15 packets. HIP connection establishment requires 4 packets (I1,R1,I2,R2) over 2 RTTs. This is beneficial for constrained environments of UAs. HIPv2 supports cryptoagility with possibility to negotiate cryptography mechanisms during the Base Exchange.

Both DTLS and HIP support mobility with a change of IP address. However, in DTLS only client mobility is well supported, while in HIP either party can be mobile. The double-jump problem (simultaneous mobility) is supported in HIP with a help of Rendezvous Server (RVS) [RFC8004]. HIP can implement secure mobility with IP source address validation in 2 RTTs, and in 1 RTT with fast mobility extension.

One study comparing DTLS and IPsec-ESP performance concluded that DTLS is recommended for memory-constrained applications while IPsec-ESP for battery power-constrained [Vignesh].

6. IANA Considerations

TBD: May need ESP ciphers defined.

7. Security Considerations

Designing secure transports is challenging. Where possible, existing technologies SHOULD be used. Both ESP and DTLS have stood "the test of time" against many attack scenarios. Their use here for Net-RID and C2 do not represent new uses, but rather variants on existing deployments.

The same can be said for both key establishment, using HIPv2 and DTLS, and the actual cipher choice for per packet encryption and authentication. Net-RID and C2 do not present new challenges, rather new opportunities to provide communications security using well researched technologies.

8. Acknowledgments

Stuart Card and Adam Wiethuechter provided information on their use of HIP for C2 at the Syracuse NY UAS test corridor. This, in large measure, was the impetus to develop this document.

9. References

9.1. Normative References
9.2. Informative References


[DTLS-1.3-draft]

<http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[hip-fast-mobility]
Moskowitz, R., Card, S. W., and A. Wiethuechter, "Fast HIP Host Mobility", Work in Progress, Internet-Draft, draft-moskowitz-hip-fast-mobility-03, 3 April 2020,

[lpwan-architecture]
Pelov, A., Thubert, P., and A. Minaburo, "LPWAN Static Context Header Compression (SCHC) Architecture", Work in Progress, Internet-Draft, draft-ietf-lpwan-architecture-01, 26 November 2021,

[MAVLINK] "Micro Air Vehicle Communication Protocol", 2021,

[new-hip-crypto]
Moskowitz, R., Card, S. W., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-10, 2 August 2021,

DOI 10.17487/RFC2104, February 1997,

[RFC5266] Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)", BCP 136, RFC 5266,
DOI 10.17487/RFC5266, June 2008,


Authors’ Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

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

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

Abstract

This document describes the use of Hierarchical Host Identity Tags (HHITs) as a self-asserting and thereby trustable Identifier for use as the UAS Remote ID. HHITs include explicit hierarchy to provide Registrar discovery for 3rd-party ID attestation.

Status of This Memo

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

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

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

This Internet-Draft will expire on 18 February 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................................. 3
2. Terms and Definitions ...................................... 3
   2.1. Requirements Terminology ............................. 3
   2.2. Notation ............................................ 3
   2.3. Definitions .......................................... 3
3. Hierarchical HITs as Remote ID ............................. 5
   3.1. Remote ID as one class of Hierarchical HITs ........ 5
   3.2. Hierarchy in ORCHID Generation ..................... 5
   3.3. Hierarchical HIT Registry ........................... 6
   3.4. Remote ID Authentication using HHITs ............... 6
4. UAS ID HHIT in DNS .......................................... 6
5. Other UTM uses of HHITs .................................... 7
6. DRIP Requirements addressed ............................... 7
7. ASTM Considerations ....................................... 7
8. IANA Considerations ....................................... 7
9. Security Considerations ................................... 8
   9.1. Hierarchical HIT Trust .............................. 9
   9.2. Collision risks with Hierarchical HITs .......... 9
10. References ................................................... 9
   10.1. Normative References ............................... 9
   10.2. Informative References ............................. 10
Appendix A. EU U-Space RID Privacy Considerations .......... 12
Appendix B. The Hierarchical Host Identity Tag (HHIT) .... 12
   B.1. HHIT prefix ......................................... 13
   B.2. HHIT Suite IDs ...................................... 13
   B.3. The Hierarchy ID (HID) ............................. 13
      B.3.1. The Registered Assigning Authority (RAA) .... 13
      B.3.2. The Hierarchical HIT Domain Authority (HDA) .. 14
Appendix C. ORCHIDs for Hierarchical HITs .................. 14
   C.1. Adding additional information to the ORCHID ...... 15
   C.2. ORCHID Decoding .................................... 16
   C.3. ORCHID Encoding .................................... 16
Appendix D. Edward Digital Signature Algorithm for HITs ... 16
   D.1. HOST_ID ........................................... 17
   D.2. HIT_SUITE_LIST ..................................... 17
Appendix E. Calculating Collision Probabilities ............ 18
Acknowledgments ................................................ 18
1. Introduction

[drip-requirements] describes a UAS ID as a "unique (ID-4), non-spoofable (ID-5), and identify a registry where the ID is listed (ID-2)"); all within a 20 character Identifier (ID-1).

This document describes the use of Hierarchical HITs (HHITs) (Appendix B) as self-asserting and thereby a trustable Identifier for use as the UAS Remote ID. HHITs include explicit hierarchy to provide Registrar discovery for 3rd-party ID attestation.

HHITs are statistically unique through the cryptographic hash feature of second-preimage resistance. The cryptographically-bound addition of the Hierarchy and thus HHIT Registries [hhit-registries] provide complete, global HHIT uniqueness. This is in contrast to general IDs (e.g. a UUID or device serial number) as the subject in an X.509 certificate.

In a multi-CA PKI, a subject can occur in multiple CAs, possibly fraudulently. CAs within the PKI would need to implement an approach to enforce assurance of uniqueness.

Hierarchical HITs are valid, though non-routable, IPv6 addresses. As such, they fit in many ways within various IETF technologies.

2. Terms and Definitions

2.1. Requirements Terminology

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

2.2. Notation

| Signifies concatenation of information - e.g., X | Y is the concatenation of X and Y.

2.3. Definitions

See [drip-requirements] for common DRIP terms.
cSHAKE (The customizable SHAKE function):
   Extends the SHAKE scheme to allow users to customize their use of the function.

HI
   Host Identity. The public key portion of an asymmetric keypair used in HIP.

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

HDA (Hierarchical HIT Domain Authority):
   The 16 bit field identifying the HIT Domain Authority under an RAA.

HHIT
   Hierarchical Host Identity Tag. A HIT with extra hierarchical information not found in a standard HIT.

HID (Hierarchy ID):
   The 32 bit field providing the HIT Hierarchy ID.

HIT
   Host Identity Tag. A 128 bit handle on the HI. HITs are valid IPv6 addresses.

Keccak (KECCAK Message Authentication Code):
   The family of all sponge functions with a KECCAK-f permutation as the underlying function and multi-rate padding as the padding rule.

RAA (Registered Assigning Authority):
   The 16 bit field identifying the Hierarchical HIT Assigning Authority.

RVS (Rendezvous Server):
   The HIP Rendezvous Server for enabling mobility, as defined in [RFC8004].

SHAKE (Secure Hash Algorithm KECCAK):
   A secure hash that allows for an arbitrary output length.

XOF (eXtendable-Output Function):
   A function on bit strings (also called messages) in which the output can be extended to any desired length.
3. Hierarchical HITs as Remote ID

Hierarchical HITs are a refinement on the Host Identity Tag (HIT) of HIPv2 [RFC7401]. HHITs require a new ORCHID mechanism as described in Appendix C. HHITs for UAS ID also use the new EdDSA/SHAKE128 HIT suite defined in Appendix D (requirements GEN-2). This hierarchy, cryptographically embedded within the HHIT, provides the information for finding the UA’s HHIT registry (ID-3).

The current ASTM [F3411-19] specifies three UAS ID types:

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

TYPE-2  A CAA assigned (presumably static) ID.

TYPE-3  A UTM system assigned UUID [RFC4122], which can but need not be dynamic.

For HHITs to be used effectively as UAS IDs, F3411-19 SHOULD add UAS ID type 4 as HHIT.

3.1. Remote ID as one class of Hierarchical HITs

UAS Remote ID may be one of a number of uses of HHITs. As such these follow-on uses need to be considered in allocating the RAAs Appendix B.3.1 or HHIT prefix assignments Section 8.

3.2. Hierarchy in ORCHID Generation

ORCHIDS, as defined in [RFC7343], do not cryptographically bind the IPv6 prefix nor the Orchid Generation Algorithm (OGA) ID (the HIT Suite ID) to the hash of the HI. The justification then was attacks against these fields are DoS attacks against protocols using them.

HHITs, as defined in Appendix C, cryptographically bind all content in the ORCHID though the hashing function. Thus a recipient of a HHIT that has the underlying HI can directly act on all content in the HHIT. This is especially important to using the hierarchy to find the HHIT Registry.
3.3. Hierarchical HIT Registry

HHITs are registered to Hierarchical HIT Domain Authorities (HDAs) as described in [hhit-registries]. This registration process ensures UAS ID global uniqueness (ID-4). It also provides the mechanism to create UAS Public/Private data associated with the HHIT UAS ID (REG-1 and REG-2).

The 2 levels of hierarchy within the HHIT allows for CAAs to have their own Registered Assigning Authority (RAA) for their National Air Space (NAS). Within the RAA, the CAAs can delegate HDAs as needed. There may be other RAAs allowed to operate within a given NAS; this is a policy decision by the CAA.

3.4. Remote ID Authentication using HHITs

The EdDSA25519 Host Identity (HI) [Appendix D] underlying the HHIT is used for the Message Wrapper, Sec 4.2 [drip-auth] (requirements GEN-2). It and the HDA’s HI/HHIT are used for the Auth Certificate, sec 5.1 [drip-auth] (requirements GEN-3). These messages also establish that the UA owns the HHIT and that no other UA can assert ownership of the HHIT (GEN-1).

The number of HDAs authorized to register UAs within an NAS determines the size of the HDA credential cache a device processing the Offline Authentication. This cache contains the HDA’s HI/HHIT and HDA meta-data; it could be very small.

4. UAS ID HHIT in DNS

There are 2 approaches for storing and retrieving the HHIT from DNS. These are:

* As FQDNs in the .aero TLD.
* Reverse DNS lookups as IPv6 addresses per [RFC8005].

The HHIT can be used to construct an FQDN that points to the USS that has the Public/Private information for the UA (REG-1 and REG-2). For example the USS for the HHIT could be found via the following. Assume that the RAA is 100 and the HDA is 50. The PTR record is constructed as:

```
100.50.hhit.uas.areo IN PTR foo.uss.areo.
```

The individual HHITs are potentially too numerous (e.g. 60 - 600M) and dynamic to actually store in a signed, DNS zone. Rather the USS would provide the HHIT detail response.
The HHIT reverse lookup can be a standard IPv6 reverse look up, or it can leverage off the HHIT structure. Assume that the RAA is 10 and the HDA is 20 and the HHIT is:

```
```

An HHIT reverse lookup would be to is:

```
a69e.ad0.1952.a3ad14.28.14.2001.20.10.hhit.arpa.
```

5. Other UTM uses of HHITs

HHITs can be used extensively within the UTM architecture beyond UA ID (and USS in UA ID registration and authentication). This includes a GCS HHIT ID. It could use this if it is the source of Network Remote ID for securing the transport and for secure C2 transport [drip-secure-nrid-c2].

Observers SHOULD have HHITs to facilitate UAS information retrieval (e.g., for authorization to private UAS data). They could also use their HHIT for establishing a HIP connection with the UA Pilot for direct communications per authorization. Further, they can be used by FINDER observers, [crowd-sourced-rid].

6. DRIP Requirements addressed

This document provides solutions to GEN 1 - 3, ID 1 - 5, and REG 1 - 2.

7. ASTM Considerations

ASTM will need to make the following changes to the "UA ID" in the Basic Message:

Type 4:
This document UA ID of Hierarchical HITs (see Section 3).

8. IANA Considerations

IANA will need to make the following changes to the "Host Identity Protocol (HIP) Parameters" registries:

Host ID:
This document defines the new EdDSA Host ID (see Appendix D.1).

HIT Suite ID:
This document defines the new HIT Suite of EdDSA/cSHAKE (see Appendix D.2).
Because HHIT use of ORCHIDv2 format is not compatible with [RFC7343], IANA is requested to allocate a new 28-bit prefix out of the IANA IPv6 Special Purpose Address Block, namely 2001:0000::/23, as per [RFC6890].

9. Security Considerations

A 64 bit hash space presents a real risk of second pre-image attacks Section 9.2. The HHIT Registry services effectively block attempts to "take over" a HHIT. It does not stop a rogue attempting to impersonate a known HHIT. This attack can be mitigated by the receiver of the HHIT using DNS to find the HI for the HHIT.

Another mitigation of HHIT hijacking is if the HI owner supplies an object containing the HHIT and signed by the HI private key of the HDA.

The two risks with hierarchical HITs are the use of an invalid HID and forced HIT collisions. The use of a DNS zone (e.g. "hhit.arpa.") is a strong protection against invalid HIDs. Querying an HDA’s RVS for a HIT under the HDA protects against talking to unregistered clients. The Registry service has direct protection against forced or accidental HIT hash collisions.

Cryptographically Generated Addresses (CGAs) provide a unique assurance of uniqueness. This is two-fold. The address (in this case the UAS ID) is a hash of a public key and a Registry hierarchy naming. Collision resistance (more important that it implied second-preimage resistance) makes it statistically challenging to attacks. A registration process as in HHIT Registries [hhit-registries] provides a level of assured uniqueness unattainable without mirroring this approach.

The second aspect of assured uniqueness is the digital signing process of the HHIT by the HI private key and the further signing of the HI public key by the Registry’s key. This completes the ownership process. The observer at this point does not know WHAT owns the HHIT, but is assured, other than the risk of theft of the HI private key, that this UAS ID is owned by something and is properly registered.
9.1. Hierarchical HIT Trust

The HHIT UAS RID in the ASTM Basic Message (the actual Remote ID message) does not provide any assertion of trust. The best that might be done is 4 bytes truncated from a HI signing of the HHIT (the UA ID field is 20 bytes and a HHIT is 16). It is in the ASTM Authentication Messages as defined in [drip-auth] that provide all of the actual ownership proofs. These claims include timestamps to defend against replay attacks. But in themselves, they do not prove which UA actually sent the message. They could have been sent by a dog running down the street with a Broadcast Remote ID device strapped to its back.

Proof of UA transmission comes when the Authentication Message includes proofs for the Location/Vector Message and the observer can see the UA or that information is validated by ground multilateration [crowd-sourced-rid]. Only then does an observer gain full trust in the HHIT Remote ID.

HHIT Remote IDs obtained via the Network Remote ID path provides a different approach to trust. Here the UAS SHOULD be securely communicating to the USS (see [drip-secure-nrid-c2]), thus asserting HHIT RID trust.

9.2. Collision risks with Hierarchical HITs

The 64 bit hash size does have an increased risk of collisions over the 96 bit hash size used for the other HIT Suites. There is a 0.01% probability of a collision in a population of 66 million. The probability goes up to 1% for a population of 663 million. See Appendix E for the collision probability formula.

However, this risk of collision is within a single "Additional Information" value. Some registration process should be used to reject a collision, forcing the client to generate a new HI and thus HIT and reapplying to the registration process.

10. References

10.1. Normative References


[hhit-registries]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", Work in Progress, Internet-
10.2. Informative References


Appendix A. EU U-Space RID Privacy Considerations

EU is defining a future of airspace management known as U-space within the Single European Sky ATM Research (SESAR) undertaking. The Concept of Operation for EuRopean UTM Systems (CORUS) project proposed a low-level Concept of Operations [corus] for UAS in EU. It introduces strong requirements for UAS privacy based on European GDPR regulations. It suggests that UAs are identified with agnostic IDs, with no information about UA type, the operators or flight trajectory. Only authorized persons should be able to query the details of the flight with a record of access.

Due to the high privacy requirements, a casual observer can only query U-space if it is aware of a UA seen in a certain area. A general observer can use a public U-space portal to query UA details based on the UA transmitted "Remote identification" signal. Direct remote identification (DRID) is based on a signal transmitted by the UA directly. Network remote identification (NRID) is only possible for UAs being tracked by U-Space and is based on the matching the current UA position to one of the tracks.

The project lists "E-Identification" and "E-Registrations" services as to be developed. These services can follow the privacy mechanism proposed in this document. If an "agnostic ID" above refers to a completely random identifier, it creates a problem with identity resolution and detection of misuse. On the other hand, a classical HIT has a flat structure which makes its resolution difficult. The Hierarchical HITs provide a balanced solution by associating a registry with the UA identifier. This is not likely to cause a major conflict with U-space privacy requirements, as the registries are typically few at a country level (e.g. civil personal, military, law enforcement, or commercial).

Appendix B. The Hierarchical Host Identity Tag (HHIT)

The Hierarchical HIT (HHIT) is a small but important enhancement over the flat HIT space. By adding two levels of hierarchical administration control, the HHIT provides for device registration/ownership, thereby enhancing the trust framework for HITs.
HHITs represent the HI in only a 64 bit hash and uses the other 32 bits to create a hierarchical administration organization for HIT domains. Hierarchical HITs are "Using cSHAKE in ORCHIDs" (Appendix C). The input values for the Encoding rules are in Appendix C.1.

A HHIT is built from the following fields:

* 28 bit IANA prefix
* 4 bit HIT Suite ID
* 32 bit Hierarchy ID (HID)
* 64 bit ORCHID hash

B.1. HHIT prefix

A unique 28 bit prefix for HHITs is recommended. It clearly separates the flat-space HIT processing from HHIT processing per "Using cSHAKE in ORCHIDs" (Appendix C).

B.2. HHIT Suite IDs

The HIT Suite IDs specifies the HI and hash algorithms. Any HIT Suite ID can be used for HHITs, provided that the prefix for HHITs is different from flat space HITs. Without a unique prefix, Appendix B.1, additional HIT Suite IDs would be needed for HHITs. This would risk exhausting the limited Suite ID space of only 15 IDs.

B.3. The Hierarchy ID (HID)

The Hierarchy ID (HID) provides the structure to organize HITs into administrative domains. HIDs are further divided into 2 fields:

* 16 bit Registered Assigning Authority (RAA)
* 16 bit Hierarchical HIT Domain Authority (HDA)

B.3.1. The Registered Assigning Authority (RAA)

An RAA is a business or organization that manages a registry of HDAs. For example, the Federal Aviation Authority (FAA) could be an RAA.
The RAA is a 16 bit field (65,536 RAAs) assigned by a numbers management organization, perhaps ICANN’s IANA service. An RAA must provide a set of services to allocate HDAs to organizations. It must have a public policy on what is necessary to obtain an HDA. The RAA need not maintain any HIP related services. It must maintain a DNS zone minimally for discovering HID RVS servers.

As HHITs may be used in many different domains, RAA should be allocated in blocks with consideration on the likely size of a particular usage. Alternatively, different Prefixes can be used to separate different domains of use of HHTs.

This DNS zone may be a PTR for its RAA. It may be a zone in a HHIT specific DNS zone. Assume that the RAA is 100. The PTR record could be constructed:

100.hhit.arpa IN PTR raa.bar.com.

B.3.2. The Hierarchical HIT Domain Authority (HDA)

An HDA may be an ISP or any third party that takes on the business to provide RVS and other needed services for HIP enabled devices.

The HDA is an 16 bit field (65,536 HDAs per RAA) assigned by an RAA. An HDA should maintain a set of RVS servers that its client HIP-enabled customers use. How this is done and scales to the potentially millions of customers is outside the scope of this document. This service should be discoverable through the DNS zone maintained by the HDA’s RAA.

An RAA may assign a block of values to an individual organization. This is completely up to the individual RAA’s published policy for delegation.

Appendix C. ORCHIDs for Hierarchical HITs

This section adds the [Keccak] based cSHAKE XOF hash function from NIST SP 800-185 [NIST.SP.800-185] to ORCHIDv2 [RFC7343]. cSHAKE is a variable output length hash function. As such it does not use the truncation operation that other hashes need. The invocation of cSHAKE specifies the desired number of bits in the hash output.

This ORCHID construction includes the Prefix in the hash to protect against Prefix substitution attacks. It also provides for inclusion of additional information, in particular the hierarchical bits of the Hierarchical HIT, in the ORCHID generation. It should be viewed as an addendum to ORCHIDv2 [RFC7343].
cSHAKE is used, rather than SHAKE from NIST FIPS 202 [NIST.FIPS.202], as cSHAKE has a parameter ’S’ as a customization bit string. This parameter will be used for including the ORCHID Context Identifier in a standard fashion.

C.1. Adding additional information to the ORCHID

ORCHIDv2 [RFC7343] is currently defined as consisting of three components:

\[
\text{ORCHID} \ := \ Prefix \ | \ OGA \ ID \ | \ \text{Encode}_{96}(\ \text{Hash})
\]

where:

- **Prefix**: A constant 28-bit-long bitstring value (IANA IPv6 assigned).
- **OGA ID**: A 4-bit long identifier for the Hash function in use within the specific usage context. When used for HIT generation this is the HIT Suite ID.
- **Encode\_96()**: An extraction function in which output is obtained by extracting the middle 96-bit-long bitstring from the argument bitstring.

This addendum will be constructed as follows:

\[
\text{ORCHID} \ := \ Prefix \ | \ OGA \ ID \ | \ \text{Info} (n) \ | \ \text{Hash} (m)
\]

where:

- **Prefix (p)**: A (max 28-bit-long) bitstring value (IANA IPv6 assigned).
- **OGA ID**: A 4-bit long identifier for the Hash function in use within the specific usage context. When used for HIT generation this is the HIT Suite ID.
- **Info (n)**: n bits of information that define a use of the ORCHID. n can be zero, that is no additional information.
- **Hash (m)**: An extraction function in which output is m bits.

\[p + n + m = 124 \text{ bits}\]
With a 28 bit IPv6 Prefix, the 96 bits currently allocated to the Encode_96 function can be divided in any manner between the additional information and the hash output. Care must be taken in determining the size of the hash portion, taking into account risks like pre-image attacks. Thus 64 bits as used in Hierarchical HITs may be as small as is acceptable.

C.2. ORCHID Decoding

With this addendum, the decoding of an ORCHID is determined by the Prefix and OGA ID (HIT Suite ID). ORCHIDv2 [RFC7343] decoding is selected when the Prefix is: 2001:20::/28.

For Heirarchical HITs, the decoding is determined by the presence of the HHIT Prefix as specified in the HHIT document.

C.3. ORCHID Encoding

ORCHIDv2 has a number of inputs including a Context ID, some header bits, the hash algorithm, and the input bitstream, normally just the public key. The output is a 96 bit value.

This addendum adds a different encoding process to that currently used. The input to the hash function explicitly includes all the fixed header content plus the Context ID. The fixed header content consists of the Prefix, OGA ID (HIT Suite ID), and the Additional Information. Secondly, the length of the resulting hash is set by the rules set by the Prefix/OGA ID. In the case of Hierarchical HITs, this is 64 bits.

To achieve the variable length output in a consistent manner, the cSHAKE hash is used. For this purpose, cSHAKE128 is appropriate. The the cSHAKE function call for this addendum is:

\[ \text{cSHAKE128(Input, L, "", Context ID)} \]

Input := Prefix | OGA ID | Additional Information | HOST_ID
L := Length in bits of hash portion of ORCHID

Hierarchical HIT uses the same context as all other HIPv2 HIT Suites as they are clearly separated by the distinct HIT Suite ID.

Appendix D. Edward Digital Signature Algorithm for HITs

Edwards-Curve Digital Signature Algorithm (EdDSA) [RFC8032] are specified here for use as Host Identities (HIs).
D.1. HOST_ID

The HOST_ID parameter specifies the public key algorithm, and for elliptic curves, a name. The HOST_ID parameter is defined in Section 5.2.19 of [RFC7401].

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>EdDSA</td>
<td>13 [RFC8032] (RECOMMENDED)</td>
</tr>
</tbody>
</table>

For hosts that implement EdDSA as the algorithm, the following ECC curves are available:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Curve</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>EdDSA</td>
<td>RESERVED</td>
<td>0</td>
</tr>
<tr>
<td>EdDSA</td>
<td>EdDSA25519</td>
<td>1 [RFC8032]</td>
</tr>
<tr>
<td>EdDSA</td>
<td>EdDSA25519ph</td>
<td>2 [RFC8032]</td>
</tr>
<tr>
<td>EdDSA</td>
<td>EdDSA448</td>
<td>3 [RFC8032]</td>
</tr>
<tr>
<td>EdDSA</td>
<td>EdDSA448ph</td>
<td>4 [RFC8032]</td>
</tr>
</tbody>
</table>

D.2. HIT_SUITE_LIST

The HIT_SUITE_LIST parameter contains a list of the supported HIT suite IDs of the Responder. Based on the HIT_SUITE_LIST, the Initiator can determine which source HIT Suite IDs are supported by the Responder. The HIT_SUITE_LIST parameter is defined in Section 5.2.10 of [RFC7401].

The following HIT Suite ID is defined, and the relationship between the four-bit ID value used in the OGA ID field and the eight-bit encoding within the HIT_SUITE_LIST ID field is clarified:

<table>
<thead>
<tr>
<th>HIT Suite</th>
<th>Four-bit ID</th>
<th>Eight-bit encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED</td>
<td>0</td>
<td>0x00</td>
</tr>
<tr>
<td>EdDSA/cSHAKE128</td>
<td>5</td>
<td>0x50</td>
</tr>
</tbody>
</table>

The following table provides more detail on the above HIT Suite combinations. The input for each generation algorithm is the encoding of the HI as defined in this Appendix. The output is 96 bits long and is directly used in the ORCHID.
Table 1: HIT Suites

<table>
<thead>
<tr>
<th>Index</th>
<th>Hash function</th>
<th>HMAC</th>
<th>Signature algorithm family</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>cSHAKE128</td>
<td>KMAC128</td>
<td>EdDSA</td>
<td>EdDSA HI hashed with cSHAKE128, output is 96 bits</td>
</tr>
</tbody>
</table>

| | |

Appendix E. Calculating Collision Probabilities

The accepted formula for calculating the probability of a collision is:

\[ p = 1 - e^{-k^2/(2n)} \]

- \( p \) Collision Probability
- \( n \) Total possible population
- \( k \) Actual population

Acknowledgments

Dr. Gurtov is an adviser on Cybersecurity to the Swedish Civil Aviation Administration.

Quynh Dang of NIST gave considerable guidance on using Keccak and the NIST supporting documents. Joan Deamen of the Keccak team was especially helpful in many aspects of using Keccak.

Authors’ Addresses

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

Email: rgm@labs.htt-consult.com
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

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping
Sweden

Email: gurtov@acm.org
Abstract

This document describes how to include trust into the ASTM Remote ID specification defined in ASTM F3411-19 under a Broadcast Remote ID (RID) scenario. It defines a few different message schemes (based on the Authentication Message) that can be used to assure past messages sent by a UA and also act as an assurance for UA trustworthiness in the absence of Internet connectivity at the receiving node.

Status of This Memo

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

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

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

This Internet-Draft will expire on 20 June 2021.

Copyright Notice

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

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

Table of Contents

1. Introduction .................................................. 2
   1.1. DRIP Requirements Addressed ............................... 3
2. Terminology .................................................. 3
   2.1. Required Terminology ..................................... 3
   2.2. Definitions .............................................. 3
3. Background ................................................... 3
   3.1. Problem Space and Focus .................................. 4
   3.2. ASTM Authentication Message .............................. 4
4. DRIP Authentication Framing Formats ................................ 6
   4.1. DRIP General Frame ...................................... 6
       4.1.1. DRIP Header ........................................ 8
       4.1.2. DRIP Authentication Data ............................. 8
       4.1.3. Forward Error Correction ............................ 9
   4.2. DRIP Wrapper Frame ..................................... 10
       4.2.1. UA Hierarchical Host Identity Tag .................. 11
       4.2.2. Trust Timestamp .................................... 11
       4.2.3. Wrapped Authentication Data ........................ 12
       4.2.4. Wrapper Signature .................................. 16
   4.3. DRIP Attestation Frame .................................. 16
       4.3.1. Attestation Data ................................... 17
       4.3.2. Expiration Timestamp ............................... 18
       4.3.3. Attestation Signature ............................... 18
5. Transport Methods & Recommendations ................................ 18
   5.1. Legacy Advertisements (Bluetooth 4.X) .................... 18
   5.2. Extended Advertisements (Bluetooth 5.X and WiFi NaN) .... 19
6. ASTM Considerations ............................................ 19
7. IANA Considerations ........................................... 20
8. Security Considerations ....................................... 20
9. Acknowledgments ............................................... 20
10. Appendix A: Thoughts on ASTM Authentication Message ............ 20
11. References .................................................. 21
   11.1. Normative References ................................... 21
   11.2. Informative References ................................. 21
Authors’ Addresses ............................................... 22

1. Introduction

UA Systems (UAS) are usually in a volatile environment when it comes to communication. UA are generally small with little computational (or flying) horsepower to carry standard communication equipment. This limits the mediums of communication to few viable options.
Observer systems (e.g. smartphones and tablets) place further constraints on the communication options. The Remote ID Broadcast messages MUST be available to applications on these platforms without modifying the devices.

The ASTM standard [F3411-19] focuses on two ways of communicating to a UAS for RID: Broadcast and Network.

This document will focus on adding trust to Broadcast RID in the current (and an expanded) Authentication Message format.

1.1. DRIP Requirements Addressed

The following [drip-requirements] will be addressed:

GEN 1: Provable Ownership  This will be addressed using the Certificate Message type (Section 4.3.1.1).

GEN 2: Provable Binding  This requirement is addressed using the Wrapped ASTM Message (Section 4.2.3.1.2), Manifest Message (Section 4.2.3.2) and Message Pack Signature (Section 4.2.3.1.1) types.

GEN 3: Provable Registration  This requirement is addressed using the Certificate Message type (Section 4.3.1.1).

2. Terminology

2.1. Required Terminology

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

2.2. Definitions

See [drip-requirements] for common DRIP terms.

Aircraft: In this document whenever the word Aircraft is used it is referring to an Unmanned Aircraft (UA) not a Manned Aircraft.

3. Background
3.1. Problem Space and Focus

The current standard for Remote ID (RID) does not, in any meaningful capacity, address the concerns of trust in the UA space with communication in the Broadcast RID environment. This is a requirement that will need to be addressed eventually for various different parties that have a stake in the UA industry.

The following subsections will provide a high level reference to the ASTM standard for Authentication Messages and how their current limitations effect trust in the Broadcast RID environment.

3.2. ASTM Authentication Message
Auth Header (1 byte):
Contains Authentication Type (AuthType) and Page Number. For
DRIP Authentication AuthType is a value of 0x5.

ASTM Authentication Headers: (6 bytes)
Contains other header information for the Authentication
Message from ASTM UAS RID Standard.

Authentication Data / Signature: (109 bytes: 17+23*4)
Opaque authentication data.

Figure 1: Standard ASTM Authentication Message format
The above diagram is the format defined by ASTM [F3411-19] that is the frame which everything this document fits into. The specific details of the ASTM headers are abstracted away as they are not necessarily required for this document.

There is a 25th byte exclude in the diagrams that comes before the Auth Header. This is the ASTM Header and consists of the Protocol Version and Message Type of the given message frame/page.

4. DRIP Authentication Framing Formats

Currently the ASTM AuthType of 0x5 should be used to denote DRIP based Authentication. The max page count of the Authentication Message is increased to 10, instead of being capped at 5.

To keep consistent formatting across the different mediums (Bluetooth 4, Bluetooth 5 and Wifi NaN) and their independent restrictions the authentication data being sent is REQUIRED to fit within the first 9 pages of the Authentication Message. The final (10th) page of the message is reserved exclusively for Forward Error Correction bytes and is only present on Bluetooth 4.

4.1. DRIP General Frame
DRIP Authentication Data

Page N:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Auth Header

Forward Error Correction

DRIP Header (1 byte):

<table>
<thead>
<tr>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FEC (1 bit):

Enabled [1] or Disabled [0]. Signals if Page N is filled with XOR FEC.

DRIP AuthType (7 bits):

<table>
<thead>
<tr>
<th>DRIP AuthType</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Wrapped ASTM Message(s)</td>
<td>0</td>
</tr>
<tr>
<td>1 Wrapped ASTM Message(s)</td>
<td>1</td>
</tr>
<tr>
<td>2 Wrapped ASTM Message(s)</td>
<td>2</td>
</tr>
<tr>
<td>3 Wrapped ASTM Message(s)</td>
<td>3</td>
</tr>
<tr>
<td>4 Wrapped ASTM Message(s)</td>
<td>4</td>
</tr>
<tr>
<td>5 Wrapped ASTM Message(s)</td>
<td>5</td>
</tr>
<tr>
<td>8 Byte Manifest</td>
<td>6</td>
</tr>
<tr>
<td>4 Byte Manifest</td>
<td>7</td>
</tr>
</tbody>
</table>
4.1.1.  DRIP Header

The DRIP Header is used to signal what kind of Authentication under DRIP that the message is using and consists of two fields.

4.1.1.1.  Forward Error Correction (Bit 8)

The Most Significant Bit is used to signal if FEC is present in the final page of the Authentication Message. It MUST be set to 1 if FEC is being used. This is only enabled under Bluetooth 4 and MUST be set to 0 on Bluetooth 5 or Wifi NaN.

4.1.1.2.  DRIP AuthType (Bits 1-7)

The lower 7 bits are used as the DRIP AuthType field denoting what Authentication type is being used. There are 5 major areas carved out of the DRIP AuthType defined by the following bitmaps:

- 000 xxxx (0x00-0x0F): Wrapped Messages (16)
- 001 xxxx (0x10-0x1F): Certificates (16)
- 01x xxxx (0x20-0x3F): Private Use (32)
- 1xx xxxx (0x40-0x6F): Reserved (48)
- 111 xxxx (0x70-0x7F): Experimental Use (16)

4.1.2.  DRIP Authentication Data

This field has a maximum size of 200 bytes. If the data is less than the max and a page is only partially filled then the rest of the partially filled page must be null padded.
This section is generally filled with either the Wrapper Frame (Section 4.2) or the Attestation Frame (Section 4.3).

4.1.3.  Forward Error Correction

To help Bluetooth (specifically Bluetooth 4) achieve the goal of reliable receipt of paged messages a Forward Error Correction (FEC) scheme is introduced and MUST be used for Legacy Advertising (Bluetooth 4) and MUST NOT be used for Extended Advertising (Bluetooth 5, Wifi NaN) under DRIP.

4.1.3.1.  Encoding

A compliant implementation of this standard MUST use XOR for the FEC. When generating the parity the first byte of every Authentication Page MUST be exclude from the XOR operation. For pages 1 through N this leaves the data portion of the page while page 0 will include a number of headers along with 17 bytes of data.

To generate the parity a simple XOR operation using the previous and current page is used. For page 0, a 23 byte null pad is used for the previous page. The resulting 23 bytes of parity is appended in one full page (always the last) allowing for recovery when any single page is lost in transmission.

4.1.3.2.  Decoding

Due to the nature of Bluetooth 4 and the existing ASTM paging structure an optimization can be used. If a Bluetooth frame fails its CRC check, then the frame is dropped without notification to the upper protocol layers. From the Remote ID perspective this means the loss of a complete frame/message/page. In Authentication Messages, each page is already numbered so the loss of a page allows the receiving application to build a "dummy" page filling the Authentication Data field (and ASTM Authentication Headers fields if page 0) with nulls.

Using the same methods as encoding, an XOR operation is used between the previous and current page (a 23 byte null pad is used when page 0 is the current page). The resulting 23 bytes is the data of the missing page.

If page 0 is being reconstructed an additional check of the Page Count, to check against how many pages are actually present, MUST be performed for sanity. An additional check on the Data Length field can also be performed, but is not required.
4.1.3.3. Limitations & Recommendations

If more than one page is lost (>1/5 for 5 page messages, >1/10 for 10 page messages) than the error rate of the link is already beyond saving and the application has more issues to deal with.

In theory under Bluetooth 4 up to 15 pages Authentication could be sent (9 pages reserved to Authentication and 6 pages reserved for Forward Error Correction). It is currently recommended however for a max of 10 pages total.

4.2. DRIP Wrapper Frame

This format MUST be encapsulated by the General Frame (Section 4.1) and reside in its data field (Section 4.1.2).

Typically the DRIP Header is set in the range of 0x00 through 0x0F (FEC disabled) or 0x80 through 0x8F (FEC enabled).

```
+---------------+---------------+---------------+---------------+
|                                                               |
|                        UA Hierarchical                        |
|                       Host Identity Tag                       |
|                                                               |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
|                         Trust Timestamp                        |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
|                                                               |
|                          Authentication Data                      |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
|                                                               |
|                                                               |
|                            Signature                           |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
```
UA Hierarchical Host Identity Tag (16 bytes):
   The UAs HHIT in byte form. Hashed from the EdDSA25519 public key.

Trust Timestamp (4 bytes):
   Timestamp denoting current time plus an offset to trust message to.

Authentication Data (116 bytes):
   Opaque authentication data using DRIP format specified in the DRIP Header. 0 to 116 bytes.

Signature (64 bytes):
   Signature over preceding fields using the EdDSA25519 keypair of the UA.

Figure 4: DRIP Wrapper Frame Format

4.2.1. UA Hierarchical Host Identity Tag

To avoid needing the UAs HHIT via the ASTM Basic ID in a detached fashion the 16 byte HHIT of the UA is included in the wrapper frame.

The HHIT for the UA (and other entities in the RID and greater UTM system under DRIP) is an enhancement of the Host Identity Tag (HIT) [RFC7401] introducing hierarchy (and how they are used in UAS RID) as defined in [drip-rid].

4.2.2. Trust Timestamp

The Trust Timestamp is of the format defined in [F3411-19]. That is a UNIX timestamp offset by 01/01/2019 00:00:00. An additional offset is then added to push the timestamp a short time into the future to avoid replay attacks.

When wrapping a Vector (Position/Location) Message the payload WILL contain (by ASTM rules) constantly changing data, this includes its own timestamp. This timestamp is only 2 bytes, which is easily attacked and only expresses the 1/10th of seconds since the last hour.

Other ASTM message types, such as Basic ID and Self-ID are static messages with no changing data. To protect a replay of these signed
messages the Trust Timestamp is the field during signing to be guaranteed to change.

The offset used against the UNIX timestamp is not defined in this document. Best practices to identify a acceptable offset should be used taking into consideration the UA environment, and propagation characteristics of the messages being sent.

4.2.3. Wrapped Authentication Data

This field has a maximum of 116 bytes in length.

4.2.3.1. Wrapped ASTM Message Formats

When wrapping any ASTM Messages and filling the Wrapped Authentication Data field under DRIP the messages MUST be in Message Type order as defined by ASTM. All message types except Authentication (0x2) and Message Pack (0xF) are allowed.

4.2.3.1.1. 0 Wrapped ASTM Message(s)

This payload type MUST only be used under Extended Advertisement (Bluetooth 5.X and Wifi NaN).

The Wrapped Authentication Data is the concatenation of all messages in the Message Pack (excluding Authentication) in Message Type order. No actual data payload is present in this format as the data is found outside the Authentication Message in the same Message Pack.

The DRIP Header is set to 0x00 (0).

4.2.3.1.2. 1 to 4 Wrapped ASTM Message(s)

This payload type can be used on either Legacy or Extended Advertisements.

The DRIP Header is set to 0x81-0x84 (129-134) when using Legacy Advertisements (FEC is enabled) and 0x01-0x04 (1-4) when using Extended Advertisements (FEC is disabled).

4.2.3.1.3. 5 Wrapped ASTM Message(s)

Editors Note: This payload type does not currently fit in the 116 byte limit of the Wrapper Frame. If the ASTM relaxes the Max Page Count limit for Legacy Advertisements to use all 15 pages then this is possible.
This payload type MUST only be used on Legacy Advertisements (Bluetooth 4.X). It requires 11 pages to complete.

The DRIP Header is set to 0x85 (133).

This payload type allows in Legacy Advertisements to have a pseudo-Message Pack like what is found in Extended Advertisements.

4.2.3.1.4. Limitations

When wrapping a single ASTM Message the 25 byte payload actually causes an inefficiency in the framing format, create a whole page unused except for a single byte. This can be optimized by removing a single byte out of the wrapped message but creates an issue on the receiver of knowing which byte was removed.

When sending a Location Message (Message Type 0x1) a single byte can be removed at the end of the message as it is currently unused. Many other messages in the ASTM Message set however do not have this ability. The first byte can not be removed as it is the key to know how to decode the message.

4.2.3.2. Manifests

Manifests fill the Wrapped Authentication Data field with hashes of previously send messages.

By hashing previously sent messages and signing them we gain trust in UAs previous reports. An observer who has been listening for any considerable length of time can hash received messages and cross check against listed hashes.

4.2.3.2.1. Hash Algorithm and Operation

The hash algorithm used for the Manifest Message is the same hash algorithm used in creation of the HHIT that is signing the Manifest.

A standard HHIT would be using cSHAKE128 from [NIST.SP.800-185]. With cSHAKE128, the hash is computed as follows:

cSHAKE128(MAC Address|Message, 8*H-Len, "", "RemoteID Auth Hash")

The message MAC Address of the transmitter is prepended to the message, as the MAC Address is the only information that links UA messages from a specific UA.

Editors Note: It should be noted that for Bluetooth mediums this is valid - however Wifi NaN does not give the receiver device the
transmitters MAC Address - making this impossible. Either MAC Address should be removed entirely or something different be used in its place to link to a given UA. Thanks Soren Friis for pointing this out.

4.2.3.2.2. 8 Byte

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash of Previous Manifest</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Hash of Current Manifest</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Message Hash 1</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Message Hash 2</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Message Hash 12</td>
</tr>
</tbody>
</table>

DRIP Header:
  With FEC: 0x87 [135] (RECOMMENDED)
  Without FEC: 0x07 [7]

Hash of Previous Manifest: (8 bytes)
  A hash of the previously sent Authentication message.

Hash of Current Manifest: (8 bytes)
  A hash of the current Authentication message.

Message Hash: (8 bytes)
  A hash of a previously sent message. 12 max.

Figure 5: 4 Byte Manifest

4.2.3.2.3. 4 Byte
Two special hashes are included in all Manifest messages; a previous manifest hash, which links to the previous manifest message, as well as a current manifest hash. This gives a pseudo-blockchain provenance to the manifest message that could be traced back if the observer was present for extended periods of time.

Creation: During creation and signing of this message format this field MUST be set to 0. So the signature will be based on this field being 0, as well as its own hash. It is an open question of if we compute the hash, then sign or sign then compute.

Cycling: There a few different ways to cycle this message. We can "roll up" the hash of 'current' to 'previous' when needed or to
completely recompute the hash. This mostly depends on the previous note.

4.2.3.2.5. Manifest Limitation

A potential limitation to this format is dwell time of the UA. If the UA is not sticking to a general area then most likely the Observer will not obtain many (if not all) of the messages in the manifest. Without the original messages received no verification can be done. Examples of such scenarios include delivery or survey UA.

4.2.4. Wrapper Signature

The wrapper signature is generated using the private key half of the UAs Host Identity (HI) and is done over all preceding data. ASTM/DRIP Headers are exclude from this operation only information within the Wrapper Fame (Section 4.2) is signed.

4.3. DRIP Attestation Frame

This format MUST be encapsulated by the General Frame (Section 4.1) and reside in its data field (Section 4.1.2).

This format is typically used to form a complete certificate using attestation data from a Registry defined in [identity-claims]. The DRIP Header is normally in the range of 0x10 through 0x1F (FEC disable) or 0x90 through 0x9F (FEC enabled).
Attestation Data: (up to 132 bytes):
   Data the UA asserts claim to.
   Up to 132 bytes in length.

Expiration Timestamp (4 bytes):
   Generated by the UA to protect against replay attacks.

Signature (64 bytes):
   Signature over preceding fields using the EdDSA25519 keypair of the UA.

Figure 7: DRIP Attestation Format

4.3.1. Attestation Data

Any data up to 132 bytes in length that the UA wishes to assert truth to.
4.3.1.1. DRIP Certificate

This payload type can be used in either Legacy or Extended Advertising. It is used to grant the ability to authenticate UA Remote ID when the receiving device of the observer (e.g. a smartphone with a dedicated RID application) has no Internet service (e.g. LTE signal).

The DRIP Header is set to 0x90 (144) when used for Legacy Advertisements and 0x10 (16) for Extended Advertisements.

The Attestation Data field is filled with the Attestation: Registry on Aircraft (Section 3.2.2 Attestation: X on Y (Offline Form) from [identity-claims]). This is binding claim between the Registry and the Aircraft, asserting the relationship between the two entities. It also provides the UA Host Identity to allow signature verification of messages signed by the UA. Also included in its structure is the HHIT of the Registry to check the local shortlist of Registries that the Observer device trusts (mapping HHITs to HIS).

More details about this Attestation and other certificates and the provisioning process can be found in [identity-claims].

4.3.2. Expiration Timestamp

Generated by the UA during the creation of the Authentication message. It is set a short time into the future to protect against replay attacks of this DRIP format.

It shares the same format as the Trust Timestamp (Section 4.2.2).

4.3.3. Attestation Signature

Performed by the UA using the onboard keypair which matches the HHIT in the Basic ID Message (0x0).

5. Transport Methods & Recommendations

5.1. Legacy Advertisements (Bluetooth 4.X)

With Legacy Advertisements the goal is to attempt to bring reliable receipt of the paged Authentication Message. Forward Error Correction (Section 4.1.3) MUST be enabled when using Legacy Advertising methods (such as Bluetooth 4.X).

Under ASTM Bluetooth 4.X rules, transmission of dynamic messages are at least every 1 second while static messages (which is what
Authentication is classified under) are sent at least every 3 seconds.

Under DRIP the Certificate Message MUST be transmitted to properly meet the GEN 1 and GEN 3 requirement.

The ASTM Message Wrapper and Manifest both satisfy the GEN 2 requirement. At least one MUST be implemented to comply with the GEN 2 requirement.

A single Manifest can carry at most (using the full 10 page limit and 8 byte hashes) 12 unique hashes of previously sent messages (of any type). This results in a total of 22 \((12 + 10)\) frames of Bluetooth data being transmitted over Bluetooth.

In comparison the Message Wrapper sends 6 pages (each a single frame) for each wrapped message. For backwards compatibility the implementation should also send the standard ASTM message that was wrapped for non-DRIP compliant receivers to obtain. This method results in 84 total Bluetooth frames \((12 + (12 * 6))\) sent.

The question of which is better suited is up to the implementation.

5.2. Extended Advertisements (Bluetooth 5.X and Wifi NaN)

Under the ASTM specification, Bluetooth 5 or Wifi NaN transport of Remote ID is to use the Message Pack (Type 0xF) format for all transmissions. Under Message Pack all messages are sent together (in Message Type order) in a single Bluetooth frame (up to 9 single frame equivalent messages). Message Packs are required by ASTM to be sent at a rate of 1 per second (like dynamic messages).

Without any fragmentation or loss of pages with transmission Forward Error Correction (Section 4.1.3) MUST NOT be used as it is impractical.

6. ASTM Considerations

* Increase Authentication Max Page Count from 5 to 10. Legacy Advertising can use all 10 while Extended Advertising has a maximum of 9 due to Bluetooth 5 limitations.

* Allocate Authentication Type 0x5 for DRIP from ASTM AuthType field.
7. IANA Considerations

This document does not require any actions by IANA.

8. Security Considerations

TODO

(Ed. Note: Hash lengths (length vs strength/collision rate); replay attacks with timestamps; static Cra (issue but nulled if UA signing other stuff dynamically meaning signatures will fail as HI won’t match - this is probably a deeper discussion topic for provisioning security considerations when we get to there))

9. Acknowledgments

Ryan Quigley and James Mussi of AX Enterprize, LLC for early prototyping to find holes in the draft specifications.

10. Appendix A: Thoughts on ASTM Authentication Message

The format standardized by the ASTM is designed with a few major considerations in mind, which the authors of this document feel put significant limitations on the expansion of the standard.

The primary consideration (in this context) is the use of the Bluetooth 5.X Extended Frame format. This method allows for a 255 byte payload to be sent in what the ASTM refers to as a "Message Pack".

The idea is to include up to five standard ASTM Broadcast RID messages (each of which are 25 bytes) plus a single authentication message (5 pages of 25 bytes each) in the Message Pack. The reasoning is then the Authentication Message is for the entire Message Pack.

The authors have no issues with this proposed approach; this is a valid format to use for the Authentication Message provided by the ASTM. However, by limiting the Authentication Message to ONLY five pages in the standard it ignores the possibility of other formatting options to be created and used.

Another issue with this format, not fully addressed in this document is fragmentation. Under Bluetooth 4.X, each page is sent separately which can result in lose of pages on the receiver. This is disastrous as the loss of even a single page means any signature is incomplete.
With the current limitation of 5 pages, Forward Error Correction (FEC) is nearly impossible without sacrificing the amount of data sent. More pages would allow FEC to be performed on the Authentication Message pages so loss of pages can be mitigated.

All these problems are further amplified by the speed at which UA fly and the Observer’s position to receive transmissions. There is no guarantee that the Observer will receive all the pages of even a 5 page Authentication Message in the time it takes a UA to traverse across their line of sight. Worse still is that not including other UA in the area, which congests the spectrum and could cause further confusion attempting to collate messages from various UA. This specific problem is out of scope for this document and our solutions in general, but should be noted as a design consideration.

11. References

11.1. Normative References


11.2. Informative References


Authors’ Addresses

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

Email: adam.wiethuechter@axenterprize.com

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

Email: stu.card@axenterprize.com

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

Email: rgm@labs.htt-consult.com