drip
Internet-Draft
Intended status: Informational
Expires: 25 July 2021

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao (Editor)
Tencent
A. Gurtov
Linkoeping University
21 January 2021

Drone Remote Identification Protocol (DRIP) Architecture
draft-ietf-drip-arch-08

Abstract

This document defines an architecture for protocols and services to support Unmanned Aircraft System Remote Identification and tracking (UAS RID), plus RID-related communications, including required architectural building blocks and their interfaces.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes an architecture for protocols and services to support Unmanned Aircraft System Remote Identification and tracking (UAS RID), plus RID-related communications, conforming to proposed regulations and external technical standards, satisfying the requirements listed in the companion requirements document [I-D.ietf-drip-reqs].

Many considerations (especially safety) dictate that UAS be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating Unmanned Aircraft Systems (UAS) Remote Identification (RID). CAAs currently (2020) promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

1.1. Overview UAS Remote ID (RID) and RID Standardization

A RID is an application enabler for a UAS to be identified by a UTM/USS or third parties entities such as law enforcement. Many safety and other considerations dictate that UAS be remotely identifiable. CAAs worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The FAA has published a Notice of Proposed Rule Making [NPRM]. CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM

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

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

3GPP

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

1.2. Overview of Types of UAS Remote ID

1.2.1. Broadcast RID

A set of RID messages are defined for direct, one-way, broadcast transmissions from the UA over Bluetooth or Wi-Fi. These are currently defined as MAC-Layer messages. Internet (or other Wide Area Network) connectivity is only needed for UAS registry information lookup by observers using the locally directly received UAS RID as a key. Broadcast RID should be functionally usable in situations with no Internet connectivity.

The Broadcast RID is illustrated in Figure 1 below.

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

Figure 1

With Broadcast RID, an Observer is limited to their radio "visible" airspace for UAS awareness and information. With Internet queries using harvested RID, the Observer may gain more information about those visible UAS.

1.2.2. Network RID

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

The Network RID is illustrated in Figure 2 below:

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

Figure 2

Via the direct Radio Frequency (RF) link between the UA and GCS, Command and Control (C2) flows between the GCS to the UA such that either can communicate with the Net-RID SP. For all but the simplest hobby aircraft, position and status flow from the UA to the GCS and on to the Net-RID SP. Thus via the Internet, through three distinct segments, Network RID information flows from the UAS to the Observer.

> Informative note: The RF link between UA and GCS is not in scope of the Network RID.

1.3. Overview of USS Interoperability

Each UAS is registered to at least one USS. With Net-RID, there is direct communication between the UAS and its USS. With Broadcast-RID, the UAS Operator has either pre-filed a 4D space volume for USS operational knowledge and/or Observers can be providing information about observed UA to a USS. USS exchange information via a Discovery and Synchronization Service (DSS) so all USS have knowledge about all activities in a 4D airspace. The interactions among observer, UA and USS is shown in Figure 3.

```
                      +----------+
                      | Observer |
                      +----------+
                     /            \
                    /              \
             +-----+                +-----+
             | UA1 |                | UA2 |
             +-----+                +-----+
                    \              /
                     \            /
                      +----------+
                      | Internet |
                      +----------+
                     /            \
                    /              \
              +-------+          +-------+
              | USS-1 | <------> | USS-2 |
              +-------+          +-------+
                       \        /
                        \      /
                        +------+
                        | DSS  |
                        +------+
```

Figure 3

1.4. Overview of DRIP Architecture

The requirements document [I-D.ietf-drip-reqs] also provides an extended introduction to the problem space, use cases, etc. Only a brief summary of that introduction will be restated here as context, with reference to the general architecture shown in Figure 4 below.

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

Figure 4

Editor's note 1: the architecture may need more clarification, and address the following:

* connectivity requirements among UA, GCS, SP, DP (if necessary)

DRIP will enable leveraging existing Internet resources (standard protocols, services, infrastructure and business models) to meet UAS RID and closely related needs. DRIP will specify how to apply IETF standards, complementing [F3411-19] and other external standards, to satisfy UAS RID requirements. DRIP will update existing and develop new protocol standards as needed to accomplish the foregoing.

This document will outline the UAS RID architecture into which DRIP must fit, and an architecture for DRIP itself. This includes presenting the gaps between the CAAs' Concepts of Operations and [F3411-19] as it relates to use of Internet technologies and UA direct RF communications. Issues include, but are not limited to:

* Mechanisms to leverage Domain Name System (DNS: [RFC1034]) and Extensible Provisioning Protocol (EPP [RFC5731]) technology to provide for private (Section 5.2) and public (Section 5.1) Information Registry.

* Trustworthy Remote ID and trust in RID messages (Section 4)

* Privacy in RID messages (PII protection) (Section 8)

  Editor's Note 2 : The following aspects are not covered in this draft, yet. We may consider add sections for each of them if necessary.

* UA -> Ground communications including Broadcast RID

* Broadcast RID 'harvesting' and secure forwarding into the UTM

* Secure UAS -> Net-RID SP communications

* Secure Observer -> Pilot communications

2. Conventions

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

3. Definitions and Abbreviations

3.1. Additional Definitions

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

3.2. Abbreviations

ADS-B: Automatic Dependent Surveillance Broadcast

DSS: Discovery & Synchronization Service

EdDSA: Edwards-Curve Digital Signature Algorithm

GCS: Ground Control Station

HHIT: Hierarchical HIT Registries

HIP: Host Identity Protocol

HIT: Host Identity Tag

RID: Remote ID

Net-RID SP: Network RID Service Provider

Net-RID DP: Network RID Display Provider.

PII: Personally Identifiable Information

RF: Radio Frequency

SDSP: Supplemental Data Service Provider

UA: Unmanned Aircraft

UAS: Unmanned Aircraft System

USS: UAS Service Supplier

UTM: UAS Traffic Management

3.3. Claims, Assertions, Attestations, and Certificates

This section introduces the meaning of "Claims", "Assertions", "Attestations", and "Certificates" in the context of DRIP.

This is due, in part, to the term "certificate" having significant technologic and legal baggage associated with it, specifically around X.509 certificates. These type of certificates and Public Key Infrastructure invokes more legal and public policy considerations than probably any other electronic communication sector. It emerged as a governmental platform for trusted identity management and was pursued in intergovernmental bodies with links into treaty instruments. As such the following terms are being used in DRIP.

Claims:

For DRIP claims are used in the form of a predicate (X is Y, X has property Y, and most importantly X owns Y). The basic form of a claim is an entity using a HHIT as an identifier in the DRIP UAS system.

Assertions:

Assertions, under DRIP, are defined as being a set of one or more claims. This definition is borrowed from JWT/CWT. An HHIT in of itself can be seen as a set of assertions. First that the identifier is a handle to an asymmetric keypair owned by the entity and that it also is part of the given registry (specified by the HID).

Attestations:

An attestation is a signed claim. The signee may be the claimant themselves or a third party. Under DRIP this is normally used when a set of entities asserts a relationship between them along with other information.

Certificates:

Certificates in DRIP have a narrow definition of being signed exclusively by a third party and are only over identities.

4. HHIT for UAS Remote ID

This section describes the basic requirements of a DRIP UAS remote ID per regulation constrains from ASTM [F3411-19] and explains the use of Hierarchical Host Identity Tags (HHITs) as self-asserting IPv6 addresses and thereby a trustable Identifier for use as the UAS Remote ID. HHITs self-attest to the included explicit hierarchy that provides Registrar discovery for 3rd-party ID attestation.

4.1. UAS Remote Identifiers Problem Space

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

The data communication of using Broadcast RID faces extreme challenging due to the limitation set by regulations. The ASTM [F3411-19] defines the Basic RID message which is expected to contained certain RID data and the Authentication message. The Basic RID message has a maximum payload of 25 bytes and the maximum size allocated by ASTM for the RID is 20 bytes and only 3 bytes are left unused. currently, the authentication maximum payload is defined to be 224 bytes.

Standard approaches like X.509 and PKI will not fit these constraints, even using the new EdDSA An example of a technology that will fit within these limitations is an enhancement of the Host Identity Tag (HIT) of HIPv2 [RFC8032] algorithm.[RFC7401] using Hierarchical HITs (HHITs) for UAS RID is outlined in HHIT based UAS

RID [I-D.ietf-drip-rid]. As PKI with X.509 is being used in other systems with which UAS RID must interoperate (e.g. the UTM Discovery and Synchronization Service and the UTM InterUSS protocol) mappings between the more flexible but larger X.509 certificates and the HHIT based structures must be devised.

By using the EdDSA HHIT suite, self-assertions of the RID can be done in as little as 84 bytes. Third-party assertions can be done in 200 bytes. An observer would need Internet access to validate a self-assertion claim. A third-party assertion can be validated via a small credential cache in a disconnected environment. This third-party assertion is possible when the third-party also uses HHITs for its identity and the UA has the public key for that HHIT

4.2. HIT as A Trustworthy UAS Remote ID

For a Remote ID to be trustworthy in the Broadcast mode, there MUST be an asymmetric keypair for proof of ID ownership. The common method of using a key signing operation to assert ownership of an ID, does not guarantee name uniqueness. Any entity can sign an ID, claiming ownership. To mitigate spoofing risks, the ID needs to be cryptographically generated from the public key, in such a manner that it is statistically hard for an entity to create a public key that would generate (spoof) the ID. Thus the signing of such an ID becomes an attestation (compared to claim) of ownership.

HITs are statistically unique through the cryptographic hash feature of second-preimage resistance. The cryptographically-bound addition of the Hierarchy and a HHIT registration process (e.g. based on Extensible Provisioning Protocol, [RFC5730]) 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.

4.3. HHIT for Remote ID Registration and Lookup

Remote IDs need a deterministic lookup mechanism that rapidly provides actionable information about the identified UA. The ID itself needs to be the inquiry input into the lookup given the constraints imposed by some of the broadcast media. This can best be achieved by an ID registration hierarchy cryptographically embedded within the ID.

The HHIT needs to consist of a registration hierarchy, the hashing crypto suite information, and the hash of these items along with the underlying public key. Additional information, e.g. an IPv6 prefix, may enhance the HHITs use beyond the basic Remote ID function (e.g. use in HIP, [RFC7401]).

A DRIP UAS ID SHOULD be a HHIT. It SHOULD be self-generated by the UAS (either UA or GCS) and MUST be registered with the Private Information Registry (More details in Section 5.2) identified in its hierarchy fields. Each UAS ID HHIT MUST NOT be used more than once, with one exception as follows.

Each UA MAY be assigned, by its manufacturer, a single HI and derived HHIT encoded as a hardware serial number per [CTA2063A]. Such a static HHIT SHOULD be used only to bind one-time use UAS IDs (other HHITs) to the unique UA. Depending upon implementation, this may leave a HI private key in the possession of the manufacturer (see Security Considerations).

Each 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. Each UAS equipped for Network RID MUST be provisioned likewise; the private key SHOULD reside 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 MUST be provisioned with public keys of the UAS RID root registries and MAY be provisioned with public keys or certificates for subordinate registries.

Operators and Private Information Registries MUST possess and other UTM entities MAY possess UAS ID style HHITs. When present, such HHITs SHOULD be used with HIP to strongly mutually authenticate and optionally encrypt communications.

4.4. HHIT for Remote ID Encryption

The only (at time of Trustworthy Remote ID design) extant fixed length ID cryptographically derived from a public key are the Host Identity Tag [RFC7401], HITs, and Cryptographically Generated Addresses [RFC3972], CGAs. Both lack a registration/retrieval capability and CGAs have only a limited crypto agility [RFC4982]. Distributed Hash Tables have been tried for HITs [RFC6537]; this is really not workable for a globally deployed UAS Remote ID scheme.

The security of HHITs is achieved first through the cryptographic hashing function of the above information, along with a registration process to mitigate the probability of a hash collision (first registered, first allowed).

5. DRIP HHIT RID Registration and Registries

The DRIP HHIT RID registration goes beyond what is currently envisioned in UTM for the UAS to USS registration/subscription process.

UAS registries hold both public and private UAS information resulting from the UAS RID registration. Given these different uses, and to improve scalability, security and simplicity of administration, the public and private information can be stored in different registries, indeed different types of registry.

5.1. Public Information Registry

5.1.1. Background

The public registry provides trustable information such as attestations of RID ownership and HDA registration. Optionally, pointers to the repositories for the HDA and RAA implicit in the RID can be included (e.g. for HDA and RAA HHIT|HI used in attestation signing operations). This public information will principally used by observers of Broadcast RID messages. Data on UAS that only use Network RID, is only available via an observer's Net-RID DP that would tend to directly provide all public registry information directly. The observer may visually "see" these UAS, but they are silent to the observer; the Net-RID DP is the only source of information based on a query for an airspace volume. Thus there is no need for information on them in a Public Registry.

5.1.2. Proposed Approach

A DRIP public information registry MUST respond to standard DNS queries, in the definitive public Internet DNS hierarchy. It MUST support NS, MX, SRV, TXT, AAAA, PTR, CNAME and HIP RR (the last per [RFC8005]) types. If a DRIP public information registry lists, in a HIP RR, any HIP RVS servers for a given DRIP UAS ID, those RVS servers MUST restrict relay services per AAA policy; this may require extensions to [RFC8004]. These public information registries SHOULD use secure DNS transport (e.g. DNS over TLS) to deliver public information that is not inherently trustable (e.g. everything other than attestations).

5.2. Private Information Registry

5.2.1. Background

The private information required for DRIP RID is similar to that required for Internet domain name registration. This information SHOULD be available for ALL UAS, including those that only use Network RID. A DRIP RID solution can leverage existing Internet resources: registration protocols, infrastructure and business models, by fitting into an ID structure compatible with DNS names. This implies some sort of hierarchy, for scalability, and management of this hierarchy. It is expected that the private registry function will be provided by the same organizations that run USS, and likely integrated with USS.

5.2.2. Proposed Approach

A DRIP RID MUST be amenable to handling as an Internet domain name (at an arbitrary level in the hierarchy), MUST be registered in at least a pseudo-domain (e.g. .ip6.arpa for reverse lookup), and MAY be registered as a sub-domain (for forward lookup). This DNS information MAY be protected with DNSSEC. Its access SHOULD be protected with a secure DNS transport (e.g. DNS over TLS).

A DRIP private information registry MUST support essential Internet domain name registry operations (e.g. add, delete, update, query) using interoperable open standard protocols. It SHOULD support the Extensible Provisioning Protocol (EPP) and the Registry Data Access Protocol (RDAP) with access controls. It MAY use XACML to specify those access controls. It MUST be listed in a DNS: that DNS MAY be private; but absent any compelling reasons for use of private DNS, SHOULD be the definitive public Internet DNS hierarchy. The DRIP private information registry in which a given UAS is registered MUST be findable, starting from the UAS ID, using the methods specified in [RFC7484]. A DRIP private information registry MAY support WebFinger as specified in [RFC7033].

6. Harvesting Broadcast Remote ID messages for UTM Inclusion

ASTM anticipated that regulators would require both Broadcast RID and Network RID for large UAS, but allow RID requirements for small UAS to be satisfied with the operator's choice of either Broadcast RID or Network RID. The EASA initially specified Broadcast RID for UAS of essentially all UAS and is now also considering Network RID. The FAA NPRM requires both for Standard RID and specifies Network RID only for Limited RID.

One obvious opportunity is to enhance the architecture with gateways from Broadcast RID to Network RID. This provides the best of both and gives regulators and operators flexibility. It offers considerable enhancement over some Network RID options such as only reporting planned 4D operation space by the operator.

These gateways could be pre-positioned (e.g. around airports, public gatherings, and other sensitive areas) and/or crowd-sourced (as nothing more than a smartphone with a suitable app is needed). As Broadcast RID media have limited range, gateways receiving messages claiming locations far from the gateway can alert authorities or a SDSP to the failed sanity check possibly indicating intent to deceive. Surveillance SDSPs can use messages with precise date/time/position stamps from the gateways to multilaterate UA location, independent of the locations claimed in the messages (which may have a natural time lag as it is), which are entirely operator self-reported in UAS RID and UTM.

Further, gateways with additional sensors (e.g. smartphones with cameras) can provide independent information on the UA type and size, confirming or refuting those claims made in the RID messages. This Crowd Sourced Remote ID (CS-RID) would be a significant enhancement, beyond baseline DRIP functionality; if implemented, it adds two more entity types.

6.1. The CS-RID Finder

A CS-RID Finder is the gateway for Broadcast Remote ID Messages into the UTM. It performs this gateway function via a CS-RID SDSP. A CS-RID Finder must implement, integrate, or accept outputs from, a Broadcast RID receiver. It MUST NOT interface directly with a GCS, Net-RID SP, Net-RID DP or Network RID client. It MUST present a TBD interface to a CS-RID SDSP; this interface SHOULD be based upon but readily distinguishable from that between a GCS and a Net-RID SP.

6.2. The CS-RID SDSP

A CS-RID SDSP MUST appear (i.e. present the same interface) to a Net-RID SP as a Net-RID DP. A CS-RID SDSP MUST appear to a Net-RID DP as a Net-RID SP. A CS-RID SDSP MUST NOT present a standard GCS-facing interface as if it were a Net-RID SP. A CS-RID SDSP MUST NOT present a standard client-facing interface as if it were a Net-RID DP. A CS-RID SDSP MUST present a TBD interface to a CS-RID Finder; this interface SHOULD be based upon but readily distinguishable from that between a GCS and a Net-RID SP.

7. DRIP Transactions Enabling Trustworthy

The UTM (U-SPACE) architecture leaves much about all the operators/ UAS to the various USS. Each CAA will have some registration requirements on operators (FAA part 105 is considered very minimal by some CAA), along with some UAS and operation registration. DRIP leverages this model with Identities for each component that augment the DRIP RID and transactions to support these Identities.

To this end, in DRIP, each Operator MUST generate a Host Identity of the Operator (HIo) and derived Hierarchical HIT of the Operator (HHITo). These are registered with a Private Information Registry along with whatever Operator data (inc. PII) is required by the cognizant CAA and the registry. In response, the Operator will obtain a Certificate from the Registry, an Operator (Cro), signed with the Host Identity of the Registry private key (HIr(priv)) proving such registration.

An Operator may now add a UA.

* An Operator MUST generate a Host Identity of the Aircraft (HIa) and derived Hierarchical HIT of the Aircraft (HHITa)

* Create a Certificate from the Operator on the Aircraft (Coa) signed with the Host Identity of the Operator private key (HIo(priv)) to associate the UA with its Operator

* Register them with a Private Information Registry along with whatever UAS data is required by the cognizant CAA and the registry

* Obtain a Certificate from the Registry on the Operator and Aircraft ("Croa") signed with the HIr(priv) proving such registration

* And obtain a Certificate from the Registry on the Aircraft (Cra) signed with HIr(priv) proving UA registration in that specific registry while preserving Operator privacy.

The operator then MUST provision the UA with HIa, HIa(priv), HHITa and Cra.

* UA engaging in Broadcast RID MUST use HIa(priv) to sign Auth Messages and MUST periodically broadcast Cra.

* UAS engaging in Network RID MUST use HIa(priv) to sign Auth Messages.

* Observers MUST use HIa from received Cra to verify received Broadcast RID Auth messages.

* Observers without Internet connectivity MAY use Cra to identify the trust class of the UAS based on known registry vetting.

* Observers with Internet connectivity MAY use HHITa to perform lookups in the Public Information Registry and MAY then query the Private Information Registry which MUST enforce AAA policy on Operator PII and other sensitive information

8. Privacy for Broadcast PII

Broadcast RID messages may contain PII. A viable architecture for PII protection would be symmetric encryption of the PII using a key known to the UAS and its USS. An authorized Observer may send the encrypted PII along with the Remote ID (to their UTM Service Provider) to get the plaintext. Alternatively, the authorized Observer may receive the key to directly decrypt all future PII content from the UA.

PII SHOULD protected unless the UAS is informed otherwise. This may come from operational instructions to even permit flying in a space/ time. It may be special instructions at the start or during an operation. PII protection should 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.

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

9. Security Considerations

The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. A manufacturer that embeds a private key in an UA may have retained a copy. A manufacturer whose UA are configured by a closed source application on the GCS which communicates over the Internet with the factory may be sending a copy of a UA or GCS self-generated key back to the factory. Keys may be extracted from a GCS or UA; the RID sender of a small harmless UA (or the entire UA) could be carried by a larger dangerous UA as a "false flag." Compromise of a registry private key could do widespread harm. Key revocation procedures are as yet to be determined. These risks are in addition to those involving Operator key management practices.

10. Acknowledgements

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM and proposed IETF DRIP WG efforts. The work of ASTM F38.02 in balancing the interests of diverse stakeholders is essential to the necessary rapid and widespread deployment of UAS RID. IETF volunteers who have contributed to this draft include Amelia Andersdotter and Mohamed Boucadair.

11. References

11.1. Normative References

[I-D.ietf-drip-reqs]
Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-06, 1 November 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-reqs-06.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

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

[Delegated]
European Union Aviation Safety Agency (EASA), "EU Commission Delegated Regulation 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems", 2019.

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

[I-D.ietf-drip-rid]
Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-rid-06, 31 December 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-rid-06.txt>.

[Implementing]
European Union Aviation Safety Agency (EASA), "EU Commission Implementing Regulation 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft", 2019.

[LAANC] United States Federal Aviation Administration (FAA), "Low Altitude Authorization and Notification Capability", n.d., <https://www.faa.gov/uas/programs_partnerships/data_exchange/>.

[NPRM] United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", 2019.

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

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

[RFC4982] Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, DOI 10.17487/RFC4982, July 2007, <https://www.rfc-editor.org/info/rfc4982>.

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

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

[RFC6537] Ahrenholz, J., "Host Identity Protocol Distributed Hash Table Interface", RFC 6537, DOI 10.17487/RFC6537, February 2012, <https://www.rfc-editor.org/info/rfc6537>.

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

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC7484] Blanchet, M., "Finding the Authoritative Registration Data (RDAP) Service", RFC 7484, DOI 10.17487/RFC7484, March 2015, <https://www.rfc-editor.org/info/rfc7484>.

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

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

[TS-22.825] 3GPP, "UAS RID requirement study", n.d., <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3527>.

[U-Space] European Organization for the Safety of Air Navigation (EUROCONTROL), "U-space Concept of Operations", 2019, <https://www.sesarju.eu/sites/default/files/documents/u-space/CORUS%20ConOps%20vol2.pdf>.

Appendix A. Overview of Unmanned Aircraft Systems (UAS) Traffic

A.1. Operation Concept

The National Aeronautics and Space Administration (NASA) and FAAs' effort of integrating UAS's operation into the national airspace system (NAS) leads to the development of the concept of UTM and the ecosystem around it. The UTM concept was initially presented in 2013. The eventual development and implementation are conducted by the UTM research transition team which is the joint workforce by FAA and NASA. World efforts took place afterward. The Single European Sky ATM Research (SESAR) started the CORUS project to research its UTM counterpart concept, namely [U-Space]. This effort is led by the European Organization for the Safety of Air Navigation (Eurocontrol).

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

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

A.2. UAS Service Supplier (USS)

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

The FAA works with UAS industry shareholders and promotes the Low Altitude Authorization and Notification Capability [LAANC] program which is the first implementation to realize UTM's functionality. The LAANC program can automate the UAS's fly plan application and approval process for airspace authorization in real-time by checking against multiple aeronautical databases such as airspace classification and fly rules associated with it, FAA UAS facility map, special use airspace, Notice to airman (NOTAM) and Temporary flight rule (TFR).

A.3. UTM Use Cases for UAS Operations

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

1. For a UAS participating in UTM and takeoff or land in a controlled airspace (e.g., Class Bravo, Charlie, Delta and Echo in United States), the USS where UAS is currently communicating with is responsible for UAS's registration, authenticating the UAS's fly plan by checking against designated UAS fly map database, obtaining the air traffic control (ATC) authorization and monitor the UAS fly path in order to maintain safe boundary and follow the pre-authorized route.

2. For a UAS participating in UTM and take off or land in an uncontrolled airspace (ex. Class Golf in the United States), pre-fly authorization must be obtained from a USS when operating beyond-visual-of-sight (BVLOS) operation. The USS either accepts or rejects received intended fly plan from the UAS. Accepted UAS operation may share its current fly 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 monitor.

A.4. Automatic Dependent Surveillance Broadcast (ADS-B)

The ADS-B is the de facto technology used in manned aviation for sharing location information, which is a ground and satellite based system designed in the early 2000s. Broadcast RID is conceptually similar to ADS-B. However, for numerous technical and regulatory reasons, ADS-B itself is not suitable for low-flying small UA. Technical reasons include: needing RF-LOS to large, expensive (hence scarce) ground stations; needing both a satellite receiver and 1090 MHz transceiver onboard CSWaP constrained UA; the limited bandwidth of both uplink and downlink, which are adequate for the current manned aviation traffic volume, but would likely be saturated by large numbers of UAS, endangering manned aviation; etc. Understanding these technical shortcomings, regulators world-wide have ruled out use of ADS-B for the small UAS for which UAS RID and DRIP are intended.

Authors' Addresses

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

Email: stu.card@axenterprize.com

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

Email: adam.wiethuechter@axenterprize.com

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

Email: rgm@labs.htt-consult.com

Shuai Zhao
Tencent
2747 Park Blvd
Palo Alto, 94588
United States of America

Email: shuai.zhao@ieee.org

Andrei Gurtov
Linkoeping University
IDA
SE-58183 Linkoeping Linkoeping
Sweden

Email: gurtov@acm.org

DRIP
Internet-Draft
Intended status: Informational
Expires: 5 May 2021

S. Card, Ed.
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
A. Gurtov
Linköping University

1 November 2020

Drone Remote Identification Protocol (DRIP) Requirements
draft-ietf-drip-reqs-06

Abstract

This document defines terminology and requirements for Drone Remote Identification Protocol (DRIP) Working Group protocols to support Unmanned Aircraft System Remote Identification and tracking (UAS RID) for security, safety and other purposes. Complementing external technical standards as regulator-accepted means of compliance with UAS RID regulations, DRIP will:

facilitate use of existing Internet resources to support UAS RID and to enable enhanced related services;

enable online and offline verification that UAS RID information is trustworthy.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction (Informative)

1.1. Motivation

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 GNSS waypoint to waypoint in a weak form of autonomy; stronger autonomy is coming. UA are "low observable": they typically have small radar cross sections; they make noise quite noticeable at short range but difficult to detect at distances they can quickly close (500 meters in under 17 seconds at 60 knots); they typically fly at low altitudes (for the small UAS to which RID applies in the US, under 400 feet AGL); they 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. Numerous other applications can be enabled or facilitated by RID: consider the importance of identifiers in many Internet protocols and services. The general scenario is illustrated in Figure 1.

```
                        UA1               UA2
                        x x               x x
                       xxxxx             xxxxx

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

Figure 1: "General UAS RID Scenario"

Note the absence of any links to/from the UA in Figure 1. This is because UAS RID and other connectivity involving the UA varies as described below.

Inherently, any responsible Observer of UA must classify them, as illustrated notionally in Figure 2. For basic airspace Situational Awareness (SA), an Observer who classifies an 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. These classes are not standard, but derive from first principles.

```
                        xxxxxxx       +--------------+
                       x       x  No  |              |
                      x   ID?   x+---->| UNIDENTIFIED |
                       x       x      |              |
                        xxxxxxx       +--------------+
                           +
                           | Yes
                           v
                        xxxxxxx
                       x       x
           +---------+x  TYPE?  x+----------+
           |           x       x            |
           |            xxxxxxx             |
           |               +                |
           v               v                v
   +--------------+ +--------------+ +--------------+
   |              | |              | |              |
   |   TASKABLE   | | LOW CONCERN  | | HIGH CONCERN |
   |              | |              | |              |
   +--------------+ +--------------+ +--------------+
```

Figure 2: "Notional UAS Classification"

An ID is not an end in itself; it exists to enable lookups and provision of services complementing mere identification.

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) Notice of Proposed Rule Making [NPRM]. However, applications of RID beyond RID itself, including DAA, have been declared out of scope in ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041 (source of the widely cited [F3411-19]), based on a distinction between RID as a security standard vs DAA as a safety application. 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 proposed regulations or technical specifications.

[Opinion1] and [WG105] cite the Direct Remote Identification previously required and specified, explicitly stating that whereas Direct RID is primarily for security purposes, "Electronic Identification" (or the "Network Identification Service" in the context of U-space) 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 EU U-space concept, as being developed in the Single European Sky ATM Research (SESAR) Joint Undertaking, whose U-space architectural principles are outlined in [InitialView].

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; enable authorities, from such an ID, to look up information about the UAS and its operator. Safety oriented UAS RID has stronger requirements. Aviation community SDOs set a higher bar for safety than for security, especially with respect to reliability.

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 all information in UAS RID is operator self-reports. Reports may be initiated by the remote pilot at the Ground Control Station (GCS) console, by a software process on the GCS, or by a process on the UA. Data in the reports may come from the UA (e.g. an on-board GNSS receiver), the GCS (e.g. dead reckoning UA location based on takeoff location and piloting commands given since takeoff) and/or sensors available to the operator (e.g. radar or cameras). 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.

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 per 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 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, is unspecified therein.

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by Observers of already ubiquitous mobile devices (typically smartphones and tablets). Anticipating likely 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 on the UA are challenging due to low altitude flight amidst structures and foliage over terrain, as well as the severe Cost, Size, Weight and Power (CSWaP) constraints of devices onboard UA. CSWaP is a burden not only on the designers of new UA for production and sale, but also on owners of existing UA 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, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of Observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges.

As RID must often operate with limited bandwidth, short packet payload length limits, and one-way links, 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 string (typically number) 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 Standards Development Organizations (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 early 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 goal 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 [ENISACSIRT]. Note that UAS RID must achieve near universal adoption, but DRIP can add value even if only selectively deployed, as those with jurisdiction over more sensitive airspace volumes may set a higher than generally mandated RID bar for flight in those volumes. Providing timely trustworthy identification data is also prerequisite to identity-oriented networking.

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, but the urgent motivation and clear initial focus is UAS. Existing Internet resources (protocol standards, services, infrastructure, and business models) should be leveraged. A natural Internet based architecture for UAS RID conforming to proposed regulations and external technical standards is described in a companion architecture document [drip-architecture] and elaborated in other DRIP documents; this document describes only relevant requirements and defines terminology for the set of 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 set of terms expected to be used in DRIP documents. This list is meant to be the DRIP terminology reference. 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 an UA, measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (GNSS).

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. Optional per [F3411-19] but may be required by regulations.

Basic ID Message
[F3411-19] Message Type 0. Provides UA Type, UAS ID Type and UAS ID, only. Mandatory per [F3411-19].

B-LOS
Beyond Line Of Sight (LOS). Term to be avoided due to ambiguity. See LOS.

BV-LOS
Beyond Visual Line Of Sight (V-LOS). See V-LOS.

CAA
Civil Aviation Authority. Two examples are 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]

Direct RID
: Direct Remote Identification. "a system that ensures the local broadcast of information about an UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA". [Delegated] Corresponds roughly to the Broadcast RID portion of [NPRM] Standard RID.

DSS
: Discovery and Synchronization Service. Formerly Inter-USS. 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 deconfliction of planned 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 GPS 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 per IATF, dedicated to aviation (but not just aircraft). Currently in design.

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.

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. US partial stopgap until UTM comes.

Limited RID
A mode of operation that must use Network RID, must not use Broadcast RID, and must provide pilot/GCS location only (not UA location). This mode is only allowed for UA that neither require (due to e.g. size) nor are equipped for Standard RID, operated within V-LOS and within 400 feet of the pilot, below 400 feet AGL, etc. [NPRM]

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

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 V-LOS.

MSL
Mean Sea Level. Relative altitude, above the variously defined mean sea level, typically of an UA (but in [NPRM] also for a GCS), measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (GNSS).

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 [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 [NPRM], the USS to which the UAS is subscribed ("Remote ID USS").

Network Identification Service
: EU regulatory requirement for Network RID. [Opinion1] and [WG105] Corresponds roughly to the Network RID portion of [NPRM] Standard RID.

Observer
: An entity (typically but not necessarily an individual human) who has directly or indirectly observed an UA and wishes to know something about it, starting with its ID. An observer typically is on the ground and local (within V-LOS 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. Optional per [F3411-19] but may be required by regulations.

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 this context, typically of the UAS Operator, Pilot In Command (PIC) or Remote Pilot, but possibly of an Observer or other party.

Remote Pilot
A pilot using a GCS to exercise proximate control of an 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. Noun or adjective, e.g. "RF link."

RF-LOS
RF LOS. 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 V-LOS.

RTCA
Radio Technical Commission for Aeronautics. US aviation SDO. Cooperates extensively with EUROCAE.

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. Optional per [F3411-19] but may be required by regulations.

Standard RID
A mode of operation that must use both Network RID (if Internet connectivity is available at the time in the operating area) and Broadcast RID (always and everywhere), and must provide both pilot/GCS location and UA location. This mode is required for UAS that exceed the allowed envelope (e.g. size, range) of Limited RID and for all UAS equipped for Standard RID (even if operated within parameters that would otherwise permit Limited RID). [NPRM] The Broadcast RID portion corresponds roughly to EU Direct RID; the Network RID portion corresponds roughly to EU Network Identification Service.

SDO
Standards Development Organization. ASTM, IETF, et al.

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., provides weather data. [FAACONOPS]

System Message
: [F3411-19] Message Type 4. Provides general UAS information, including remote pilot location, multiple UA group operational area, etc. Optional per [F3411-19] but may be required by regulations.

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", 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]

UAS ID Type
: UAS Identifier type index. 4 bits, see Section 3, Paragraph 5 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.

UAS RID Verifier Service
: System component designed to handle the authentication requirements of RID by offloading verification to a web hosted service. [F3411-19]

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" per [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, per 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.

V-LOS
Visual LOS. Typically used in describing operation of an UA by a "remote" pilot who can clearly directly (without video cameras or any other 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

Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The US FAA has described the key role that UAS RID plays in UAS Traffic Management (UTM) in [NPRM] and [FAACONOPS] (especially Section 2.6 of the latter). CAAs currently (2020) promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM developed a widely cited Standard Specification for Remote ID and Tracking [F3411-19] (early drafts are freely available as [OpenDroneID] specifications). It 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 layer), to be received in real time by local Observers.

UAS using both means must send the same UAS RID application layer information via each per [F3411-19] and [NPRM]. 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 for UAS registry information lookup using the directly locally received UAS Identifier (UAS ID) as a key. Broadcast RID does not assume IP connectivity of UAS; messages are encapsulated by the UA without IP, directly in Bluetooth or WiFi link layer frames.

[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 (generally static) ID, like the registration number of a manned aircraft.

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

Per [Delegated], the EU allows only Type 1. Per [NPRM], the US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once as a "Session ID" (for a single UAS flight, which in the context of UTM is called an "operation"). Per [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. Per [NPRM], the US allows but does not require that operator registration numbers be sent. As yet apparently there are no CAA public proposals to use Type 2.

3.1. Network RID

```
             x x    UA
            xxxxxxx
             |    \
             |     \
             |      \
             |       \  ********************
             |        \*              ------*---+------------+
             |        *\             /       *  | NET_Rid_SP |
             |        * ------------/    +---*--+------------+
             | RF     */                 |   *
             |        /     INTERNET     |   *  +------------+
             |       /*                  +---*--| NET_Rid_DP |
             |      / *                 +----*--+------------+
             +     /   *                |   *
              x   /     ****************|***      x
            xxxxx                       |       xxxxx
              x                         +-------  x
              x                                   x
             x x   Operator's GCS     Observer   x x
            x   x                               x   x
```

Figure 3: "Network RID Information Flow"

Only two of the three links UA-GCS, UA-Internet and GCS-Internet need exist, although all three may. There must be some 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) information to the GCS. There 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 Net-RID SP.

Currently, the RID data flow typically originates on the UA and passes through the GCS, or originates on the GCS, rather than comes direct from the UA as in Broadcast RID (below), and makes up to three trips through the Internet, implying use of IP (and other middle layer protocols) on those trips, but not necessarily on an UA-GCS link (if indeed that direct even exists and further the Network RID data flows across it).

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 an 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 unspecified (generally presumed to be web browser based) means.

Network RID has several variants. The UA may have persistent onboard Internet connectivity, in which case it can consistently source RID information directly over the Internet. The UA may have intermittent onboard Internet connectivity, in which case the GCS must source RID information whenever the UA itself is offline. The UA may not have Internet connectivity of its own, but have instead some other form of communications to another node that can relay RID information to the Internet; this would typically be the GCS (which to perform its function must know where the UA is, although C2 link outages do occur).

The UA may have no means of sourcing RID information, in which case the GCS must source it; this is typical under FAA NPRM Limited RID proposed rules, which require providing the location of the GCS (not that of the UA). In the extreme case, this could be the pilot using a web browser/application to designate, to an UAS Service Supplier (USS) or other UTM entity, a time-bounded airspace volume in which an operation will be conducted; this may impede disambiguation of ID if multiple UAS operate in the same or overlapping 4-D volumes.

In most cases in the near term, if the RID information is fed to the Internet directly by the UA or GCS, the first hop data links will be cellular Long Term Evolution (LTE) or Wi-Fi, but provided the data link can support at least UDP/IP and ideally also TCP/IP, its type is generally immaterial to the higher layer protocols. An UAS as the ultimate source of Network RID information feeds an USS acting as a Network RID Service Provider (Net-RID SP), which essentially proxies for that and other sources; an observer or other ultimate consumer of Network RID information obtains it from a Network RID Display Provider (Net-RID DP), 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, accessible via typical means such as web APIs/ browsers.

Network RID is the more flexible and less constrained of the defined UAS RID means, but is only partially specified in [F3411-19]. It is presumed that IETF efforts supporting Broadcast RID (see next section) can be easily generalized for Network RID.

3.2. Broadcast RID

```
 x x  UA
xxxxx
  |
  |
  | app messages directly over one-way RF data link
  |
  |
  +
  x
xxxxx
  x
  x
 x x   Observer's device (e.g. smartphone)
x   x
```

Figure 4: "Broadcast RID Information Flow"

Note the absence of the Internet from this information flow sketch. This is because Broadcast RID is one-way direct transmission of application layer messages over a RF data link (without IP or other middle layer protocols) 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 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 and FAA have not indicated intent to allow, and FAA has proposed explicitly to prohibit, use of ADS-B for UAS RID.

[F3411-19] specifies three Broadcast RID data links: Bluetooth 4.X; Bluetooth 5.X Long Range; and Wi-Fi with Neighbor Awareness Networking (NAN). For compliance with [F3411-19], an UA must broadcast (using advertisement mechanisms where no other option supports broadcast) on at least one of these; if broadcasting on Bluetooth 5.x, it is also required concurrently to do so on 4.x (referred to in [F3411-19] as Bluetooth Legacy). Future revisions 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 Application Programming Interface (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 26 byte limit of the Bluetooth 4.X "Broadcast Frame" transmitted on beacon channels. After nominal overheads, this limits the UAS ID string to a maximum length of 20 bytes, and precludes the same frame carrying position, velocity and other information that should be bound to the UAS ID, much less strong authentication data. This requires segmentation ("paging") of longer messages or message bundles ("Message Pack"), and/or correlation of short messages (anticipated by ASTM to be done on the basis of Bluetooth 4 MAC address, which is weak and unverifiable).

[F3411-19] Broadcast RID specifies several message types: Basic, Location, Authentication, Self-ID, System and Operator ID. To satisfy EASA and FAA proposed rules, all types are needed, except Authentication and Self-ID.

[F3411-19] Broadcast RID specifies very few quantitative performance requirements: static information must be transmitted at least once per 3 seconds; dynamic information (the Location message) must be transmitted at least once per second and be no older than one second when sent. [NPRM] proposes 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. 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). 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.

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; from this point until the end of 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. Also, dynamic constraints (formerly 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. [F3411-19] etc. provide very limited choices 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 be contacted 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 unreliable. 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.

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 an 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.

4. Requirements

4.1. General

GEN-1 Provable Ownership: DRIP MUST enable verification that the UAS ID asserted in the Basic ID message is that of the actual current sender of the message (i.e. the message is not a replay attack or other spoof, authenticating e.g. by verifying an asymmetric cryptographic signature using a sender provided public key from which the asserted 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 binding 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 verification that the UAS ID is in a registry and identification of which one, even on an observer device lacking Internet connectivity at the time of observation; with UAS ID Type 3, 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.

GEN-5 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), to support three objectives: 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); defend against replay attacks; and support optional SDSP services such as multilateration (to complement UAS position self-reports with independent measurements).

GEN-6 Finger: DRIP MUST enable dynamically establishing, with AAA, per policy, end to end strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including at least the remote pilot and USS.

GEN-7 QoS: DRIP MUST enable policy based specification of performance and reliability parameters, such as maximum message transmission intervals and delivery latencies.

GEN-8 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).

GEN-9 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.

GEN-10 Multicast: DRIP SHOULD support multicast for efficient and flexible publish-subscribe notifications, e.g., of UAS reporting positions in designated airspace volumes.

GEN-11 Management: DRIP SHOULD support monitoring of the health and coverage of Broadcast and Network RID services.

Requirements imposed either by regulation or [F3411-19] are not reiterated here, but drive many of the numbered requirements listed here. The [NPRM] 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 may involve machine assisted format conversions, e.g. from binary encodings. The "gateway" requirement is the only instance in which DRIP transports [F3411-19] messages; most of DRIP pertains to the authentication of such messages and the identifier carried within them.

4.2. Identifier

ID-1 Length: The DRIP (UAS) entity (remote) identifier must be no longer than 20 bytes (per [F3411-19] to fit in a Bluetooth 4 advertisement payload).

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

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

ID-4 Uniqueness: The DRIP identifier MUST be unique within the global UAS RID 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 such as the FAA's proposed 6 months RID data retention period, revocation by the registry, or surrender by the operator).

ID-5 Non-spoofability: The DRIP identifier MUST be non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID).

ID-6 Unlinkability: A DRIP UAS ID MUST NOT facilitate adversarial correlation over multiple UAS operations; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support well-defined scalable timely registration methods.

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 (and possibly other protocols); and in RID initiated V2X applications such as DAA and C2, it could be used between the network and transport layers (with HIP or DTLS).

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 an UAS ID is generated by the operator, GCS, UA, USS or registry, or some collaboration thereamong, is unspecified; however, there must be agreement on the UAS ID among these entities.

4.3. Privacy

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, which information is public and which private. By default, all information required to be transmitted via Broadcast RID, even when actually sent via Network RID, is assumed to be public; all other information contained 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.

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

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, per 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 MUST enable closing the AAA-policy registry loop by governing AAA per registered policies and administering policies only via AAA.

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. However those may evolve, the essential registry functions remain the same, so are specified herein.

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. Potential vulnerabilities of DRIP 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 of (e.g. 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, e.g. as a "false flag", by a larger (malicious) UA

It may be inferred from the Section 4.1 General requirements for Provable Ownership, Provable Binding and Provable Registration, together with the Section 4.2 Identifier requirements, 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. E.g. 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. 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.

7. Privacy and Transparency Considerations

Privacy is closely related to but not synonymous with security, and conflicts with transparency. Privacy and transparency are important for legal reasons including regulatory consistency. [EU2018] [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 documents give due regard to [RFC6973] and more broadly [RFC8280].

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[cpdlc] Gurtov, A., Polishchuk, T., and M. Wernberg, "Controller-Pilot Data Link Communication Security", MDPI Sensors 18(5), 1636, 2018, <https://www.mdpi.com/1424-8220/18/5/1636>.

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

[Delegated] European Union Aviation Safety Agency (EASA), "Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems", March 2019.

[drip-architecture] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-arch-04, 28 October 2020, <https://tools.ietf.org/html/draft-ietf-drip-arch-04>.

[ENISACSIRT] European Union Agency for Cybersecurity (ENISA), "Actionable information for Security Incident Response", November 2014, <https://www.enisa.europa.eu/topics/csirt-cert-services/reactive-services/copy_of_actionable-information>.

[EU2018] European Parliament and Council, "2015/0277 (COD) PE-CONS 2/18", February 2018.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[FAACONOPS]
FAA Office of NextGen, "UTM Concept of Operations v2.0", March 2020.

[I-D.maeurer-raw-ldacs]
Maeurer, N., Graeupl, T., and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)", Work in Progress, Internet-Draft, draft-maeurer-raw-ldacs-06, 2 October 2020, <https://tools.ietf.org/html/draft-maeurer-raw-ldacs-06>.

[ICAOATM] International Civil Aviation Organization, "Doc 4444: Procedures for Air Navigation Services: Air Traffic Management", November 2016.

[ICAOUAS] International Civil Aviation Organization, "Circular 328: Unmanned Aircraft Systems", February 2011.

[ICAOUTM] International Civil Aviation Organization, "Unmanned Aircraft Systems Traffic Management (UTM) - A Common Framework with Core Principles for Global Harmonization, Edition 2", November 2019.

[Implementing]
European Union Aviation Safety Agency (EASA), "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft", May 2019.

[InitialView]
SESAR Joint Undertaking, "Initial view on Principles for the U-space architecture", July 2019.

[NPRM] United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019.

[OpenDroneID]
Intel Corp., "Open Drone ID", March 2019, <https://github.com/opendroneid/specs>.

[Opinion1] European Union Aviation Safety Agency (EASA), "Opinion No 01/2020: High-level regulatory framework for the U-space", March 2020.

[Recommendations]
FAA UAS Identification and Tracking Aviation Rulemaking Committee, "UAS ID and Tracking ARC Recommendations Final Report", September 2017.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

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

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[Roadmap] American National Standards Institute (ANSI) Unmanned Aircraft Systems Standardization Collaborative (UASSC), "Standardization Roadmap for Unmanned Aircraft Systems draft v2.0", April 2020, <https://share.ansi.org/Shared Documents/Standards Activities/UASSC/UASSC_20-001_WORKING_DRAFT_ANSI_UASSC_Roadmap_v2.pdf>.

[Stranger] Heinlein, R.A., "Stranger in a Strange Land", June 1961.

[WG105] EUROCAE, "WG-105 draft Minimum Operational Performance Standards (MOPS) for Unmanned Aircraft System (UAS) Electronic Identification", June 2020.

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 necessary 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 and Flightradar 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-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.

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.maeurer-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, Mohamed Boucadair, Toerless Eckert, Susan Hares, Mika Jarvenpaa, Daniel Migault, Alexandre Petrescu, Saulo Da Silva and Shuai Zhao.

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

DRIP R. Moskowitz
Internet-Draft HTT Consulting
Intended status: Standards Track S. Card
Expires: 19 May 2021 A. Wiethuechter
AX Enterprize
S. Zhao
Tencent
H. Birkholz
Fraunhofer SIT
15 November 2020

Crowd Sourced Remote ID
draft-moskowitz-drip-crowd-sourced-rid-05

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 FAA mandated Network Remote ID (N-RID) functionality. This crowd sourced B-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

Copyright Notice

Table of Contents

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 SDSP(s) 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 CAAs are placing on Network Remote ID (N-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. The SDSP will make any filtering decisions in what it forwards to the UTM(s).

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 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.

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 this is and there is not monitoring coverage. They may also use this information of where to place pro-active monitoring coverage.

An SDSP SHOULD only forward Authenticated B-RID messages like those defined in [tmrid-auth] to the UTM(s). Further, the SDSP SHOULD validate the Remote ID (RID) and the Authentication signature before forwarding anything from the UA.

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.

1.1. 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.

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.

CAA:
: Civil Aeronautics Administration. An example is the Federal Aviation Administration (FAA) in the United States of America.

DAA:
: Detect and Avoid. The process of a UA detecting obstacles, like other UAs and taking the necessary evasive action.

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.

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 GPS waypoints, or otherwise directing its flight.

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

Observer:
Referred to in other UAS documents as a "user", but there are also other classes of RID users, so we prefer "observer" to denote an individual who has observed an UA and wishes to know something about it, starting with its RID.

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.

NETSP:
Network RID Service Provider. USS receiving Network RID messages from UAS (UA or GCS), storing for a short specified time, making available to NETDP.

NETDP:
Network RID Display Provider. Entity (might be USS) aggregating data from multiple NETSPs to answer query from observer (or other party) desiring Situational Awareness of UAS operating in a specific airspace volume.

N-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.

SDSP:
Supplemental Data Service Provider. Entity providing information that is allowed, but not required to be present in the UTM system.

UA:
Unmanned Aircraft. In this document UA's are typically though of as drones of commercial or military variety. This is a very strict definition which can be relaxed to include any and all aircraft that are unmanned.

UAS:
Unmanned Aircraft System. Composed of Unmanned Aircraft and 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 the control station.

UTM:
UAS Traffic Management. A "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management (ATM) system.

USS:
UAS Service Supplier. Provide UTM 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. (From FAA UTM ConOps V1, May 2018).

3. Problem Space

3.1. Meeting the needs of Network ID

The Federal (US) Aviation Authority (FAA), in the December 31, 2019 Remote ID Notice of Proposed Rulemaking [FAA-NPRM], is requiring "Standard" and "Limited" Remote ID. Standard is when the UAS provides both Network and Broadcast RID. Limited is when the UAS provides only Network RID. The FAA has dropped their previous position on allowing for only Broadcast RID. We can guess as to their reasons; they are not spelled out in the NPRM. It may be that just B-RID does not meet the FAA's statutory UA tracking responsibility.

The UAS vendors have commented that N-RID places considerable demands on currently used UAS. For some UAS like RC planes, meaningful N-RID (via the Pilot's smartphone) are of limited value. A mechanism that can augment B-RID to provide N-RID would help all members of the UAS environment to provide safe operation and allow for new applications.

3.2. Advantages of Broadcast Remote ID

B-RID has its advantages over N-RID.

* B-RID can more readily be implemented directly in the UA. N-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 straight-forward 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 [tmrid-auth].

The SPDP can manage the number of Finders in an area (see Section 4.2) 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 [tmrid-auth] 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 Hierarchical HITS, [hierarchical-hit] and [hhit-registries].

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. HIPv2 [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. 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.

4.2. 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. 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]. The CDDL [RFC8610] specification is used for CS-RID message description

CS-RID MAC and COAP [RFC7252] for the CS-RID protocol.

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

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

The CS-RID MESSAGE CONTENT varies by MESSAGE TYPE.

5.1. CS-RID MESSAGE TYPE

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

Number	CS-RID Message Type
0	Reserved
1	B-RID Forwarding
2	Finder Registration
3	SDSP Response
4	Finder Location

Figure 1

5.1.1. 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,
}

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.

```
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"
```

Figure 4

5.2. 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
)
```

5.2.1. CS-RID ID

The CS-RID ID is the ID recognized by the SDSP. This may be an HHIT Hierarchical HITs [hierarchical-hit], or any ID used by the SDSP.

5.2.2. 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,
]
```

Figure 5

5.3. CS-RID Finder Registration

The CS-RID Finder MAY use HIPv2 [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 HIPv2 mobility functionality and ESP [RFC4303] support are not used.

When HIPv2 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 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
)
```

5.3.1. 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

5.4. CS-RID SDSP Response

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

```
 (
   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.

5.4.1. CDDL description for SDSP Response

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

```
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

5.5. CS-RID Location Update

The Finder SHOULD provide regular location updates to the SDSP. The interval is based on the Update Interval from Section 5.4 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 recieved 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
)
```

5.5.1. 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. 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,
       HF  : 5,
       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"
<CODE ENDS>
```

7. IANA Considerations

TBD

8. Security Considerations

TBD

8.1. Privacy Concerns

TBD

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

9.2. Informative References

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[FAA-NPRM] Federal (US) Aviation Authority, "FAA Remote ID Notice of Proposed Rule Making", December 2019, <https://www.regulations.gov/docket?D=FAA-2019-1100>.

[hhit-registries] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", Work in Progress, Internet-Draft, draft-moskowitz-hip-hhit-registries-02, 9 March 2020, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-hhit-registries-02.txt>.

[hierarchical-hit] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-05, 13 May 2020, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-hierarchical-hit-05.txt>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, DOI 10.17487/RFC5238, May 2008, <https://www.rfc-editor.org/info/rfc5238>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[tmrid-auth] Wiethuechter, A., Card, S., and R. Moskowitz, "TM-RID Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-tmrid-auth-05, 18 February 2020, <http://www.ietf.org/internet-drafts/draft-wiethuechter-tmrid-auth-05.txt>.

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
Tencent
2747 Park Blvd
Palo Alto, CA 94306
United States of America

Email: shuai.zhao@ieee.org

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany

Email: henk.birkholz@sit.fraunhofer.de

DRIP R. Moskowitz
Internet-Draft HTT Consulting
Intended status: Standards Track S. Card
Expires: April 26, 2021 A. Wiethuechter
AX Enterprize
October 23, 2020

UAS Operator Privacy for RemoteID Messages
draft-moskowitz-drip-operator-privacy-06

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

Copyright Notice

Table of Contents

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 [drip-requirements], 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-CFB32 mode of operation proposed here can encrypt a multiple of 4 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.

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 Drip Requirements [drip-requirements] 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.

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.

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 a 20 Character USS ID and a 256 bit random nonce to the USS. These are inputs, along with the ECDH keys to produce the shared secret as follows.

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

```
Shared Secret = KMAC128(salt, 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.

salt = Nonce-USS | Nonce-UAS

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

IKM = Diffie-Hellman secret | USS-ID | 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.

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-CFB32 is the recommended default cipher.

ASTM Remote ID and Tracking messages [F3411-19] SHOULD be updated to allow Bit 2 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 looses 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 20 bytes for Operator the 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-CFB32 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 looses 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-CFB32

CFB32 is defined in [NIST.SP.800-38A], Section 6.3. This is the Cipher Feedback (CFB) mode operating on 32 bits at a time. This variant of CFB can be used to encrypt any multiple of 4 bytes of cleartext.

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

The 128 bit IV for AES-CFB32 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-CFB32 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 pubic 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 2:
  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. CFB32 Risks

Using the same IV for different Operator information values with CFB32 presents a cyptoanalysis 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.SP.800-185]
Kelsey, J., Change, S., and R. Perlner, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[NIST.SP.800-38A]
Dworkin, M., "Recommendation for block cipher modes of operation :", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-38a, 2001, <https://doi.org/10.6028/nist.sp.800-38a>.

[NIST.SP.800-56Cr1]
Barker, E., Chen, L., and R. Davis, "Recommendation for key-derivation methods in key-establishment schemes", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-56cr1, April 2018, <https://doi.org/10.6028/nist.sp.800-56cr1>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

12. Informative References

[drip-requirements]
Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-05, October 16, 2020, <https://tools.ietf.org/html/draft-ietf-drip-reqs-05>.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/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 |-> Y, we should choose d >= 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?

```
Enc(X, K):
  1. Y <- X.
  2. Split Y into 2 equal parts: Y = Y1 || Y2
  (let us assume for simplicity that m is even).
  3. For i = 1, 2, ..., d do:
    Y <- Y2 || (Y1 ^ first_m/2_bits(E_K(Y2 || Ci)),
  where Ci is a (n - m/2)-bit round constant.
  4. Y <- Y2 || Y1.
  5. Return Y.

Dec(Y, K):
  1. X <- Y.
  2. Split X into 2 equal parts: X = X1 || X2.
  3. For i = d, ..., 2, 1 do:
    X <- X2 || (X1 ^ first_m/2_bits(E_K(X2 || Ci)).
  4. X <- X2 || X1.
  5. Return X.
```

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

DRIP R. Moskowitz
Internet-Draft HTT Consulting
Intended status: Standards Track S. Card
Expires: 28 June 2021 A. Wiethuechter
AX Enterprize
A. Gurtov
Linköping University
25 December 2020

Secure UAS Network RID and C2 Transport
draft-moskowitz-drip-secure-nrid-c2-02

Abstract

This document provides the mechanisms for secure transport of UAS Network-RemoteID and Command-and-Control messaging. Both HIP and DTLS based methods are 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 June 2021.

Copyright Notice

Table of Contents

1. Introduction

This document defines mechanisms to provide secure transport for the ASTM Network Remote ID [F3411-19] (N-RID) and UAS Command and Control (C2) messaging.

A secure transport for C2 is critical for UAS Beyond line of sight (BLOS) operations.

Two options for secure transport are provided: HIPv2 [RFC7401] and DTLS [DTLS-1.3-draft]. These options are generally defined and their applicability is compared and contrasted. It is up to N-RID and C2 to select which is preferred for their situation.

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 [drip-requirements] for common DRIP terms.

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

N-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 RID endpoints

The 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 N-RID communication flow. An Operator is expected to register an operation with the USS. If this is done via the GCS and the GCS is the source (directly acting as a gateway), this could set up the secure connection for N-RID. 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 N-RID communications.

The UAS component in N-RID may be either the UA, GCS, or the Operator’s Internet connected device (e.g. smartphone or tablet). In all cases, mobility MUST be assumed. That is the IP address of this end of the N-RID communication will change during an operation. The N-RID mechanism MUST support this. the UAS Identity for the secure connection may vary based on the UAS endpoint.

3.1. N-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. 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.

3.2. N-RID from the GCS

Many UA will lack direct Internet access, but their GCS may be so connected. There are two sources for the GCS for the RID messages, 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 (delivery van), so it can have as mobility demanding connection needs as the UA.

3.3. N-RID from the Operator

Many UAS will have no Internet connectivity, but the UA is sending B-RID messages and the Operator has an Internet Connected device that is receiving these B-RID messages. The Operator’s device can act as the proxy for these messages, turning them into N-RID messages.

3.4. UAS Identity

The UA MAY use its RID private key if the RID is a HHIT [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.

4. Command and Control

Command and Control (C2) connection is between the UA and GCS. Often this 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.

5. Secure Transports

The raw RID and C2 messages will be wrapped in UDP. These UDP packets will either be transported in ESP for the HIPv2 approach or DTLS application messages for DTLS. In both cases header compression technologies SHOULD be used and negotiated based on policy.

For IPv6 over both WiFi and Bluetooth (or any other radio link), Robust Header Compression (ROHC) [RFC5795] and/or Generic Header Compression (6LoWAN-HGC) [RFC7400] can significantly reduce the per packet transmission cost of IPv6. 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. Both WiFi and Bluetooth link security can provide appropriate security, but this would not provide trustworthy multi-homed security.

5.1. HIPv2 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 usedfor C2 HIP.

When the UA is the UAS endpoint for N-RID, and particularly when HIP is used for C2, HIP for N-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 N-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 N-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 computationally 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.

For ESP with HIP [RFC7402], an additional 4 - 8 bytes can be trimmed by using the Implicit IV for ESP option [RFC8750].

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-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

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 N-RID and C2 do not represent new uses, but rather variants on existing depoyments.

The same can be said for both key establishment, using HIPv2 and DTLS, and the actual cipher choice for per packet encryption and authentication. N-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 provivded 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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[drip-requirements] Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-06, 1 November 2020, <https://tools.ietf.org/html/draft-ietf-drip-reqs-06>.

[drip-uas-rid] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-uas-rid-06, 17 August 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-uas-rid-06>.

[DTLS-1.3-draft] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-39, 2 November 2020, <https://tools.ietf.org/html/draft-ietf-tls-dtls13-39>.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[hip-fast-mobility] Moskowitz, R., Card, S., and A. Wiethuechter, "Fast HIP Host Mobility", Work in Progress, Internet-Draft, draft-moskowitz-hip-fast-mobility-03, 3 April 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-fast-mobility-03>.

[new-crypto] Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-06, 2 November 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-new-crypto-06>.

[RFC5795] Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, DOI 10.17487/RFC5795, March 2010, <https://www.rfc-editor.org/info/rfc5795>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 7402, DOI 10.17487/RFC7402, April 2015, <https://www.rfc-editor.org/info/rfc7402>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015, <https://www.rfc-editor.org/info/rfc7668>.

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

[RFC8750] Migault, D., Guggemos, T., and Y. Nir, "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)", RFC 8750, DOI 10.17487/RFC8750, March 2020, <https://www.rfc-editor.org/info/rfc8750>.

[Vignesh] Vignesh, K., "Performance analysis of end-to-end DTLS and IPsec-based communication in IoT environments", Thesis no. MSEE-2017: 42, 2017, <http://www.diva-portal.org/smash/get/diva2:1157047/FULLTEXT02>.

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

DRIP
Internet-Draft
Intended status: Standards Track
Expires: 18 February 2021

R. Moskowitz
HTT Consulting
S. Card
A. Wiethuechter
AX Enterprize
A. Gurtov
Linköping University
17 August 2020

UAS Remote ID
draft-moskowitz-drip-uas-rid-06

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

Copyright Notice

Table of Contents

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.

HITs 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:

```
2001:14:28:14:a3ad:1952:ad0:a69e
```

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 allocated 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

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

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

Draft, draft-moskowitz-hip-hhit-registries-02, 9 March 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hhit-registries-02>.

[NIST.FIPS.202]
Dworkin, M., "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.202, July 2015, <https://doi.org/10.6028/nist.fips.202>.

[NIST.SP.800-185]
Kelsey, J., Change, S., and R. Perlner, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[corus] CORUS, "U-space Concept of Operations", September 2019, <https://www.sesarju.eu/node/3411>.

[crowd-sourced-rid]
Moskowitz, R., Card, S., Wiethuechter, A., Zhao, S., and H. Birkholz, "Crowd Sourced Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-crowd-sourced-rid-04, 20 May 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-crowd-sourced-rid-04>.

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

[drip-auth]
Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-drip-auth-03, 27 July 2020, <https://tools.ietf.org/html/draft-wiethuechter-drip-auth-03>.

[drip-requirements]
Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-03, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-drip-reqs-03>.

[drip-secure-nrid-c2]
Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "Secure UAS Network RID and C2 Transport", Work in Progress, Internet-Draft, draft-moskowitz-drip-secure-nrid-c2-00, 6 April 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-secure-nrid-c2-00>.

[Keccak] Bertoni, G., Daemen, J., Peeters, M., Van Assche, G., and R. Van Keer, "The Keccak Function", <https://keccak.team/index.html>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC7343] Laganier, J. and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)", RFC 7343, DOI 10.17487/RFC7343, September 2014, <https://www.rfc-editor.org/info/rfc7343>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

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

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

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. Concept of Operation for EuRopean UTM Systems (CORUS) project proposed 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 subsitution 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:

```
ORCHID     :=  Prefix | OGA ID | Encode_96( 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:

```
ORCHID     :=  Prefix | OGA ID | Info (n) | 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 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:

```
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].

Algorithm profiles	Values	
EdDSA	13 [RFC8032]	(RECOMMENDED)

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

Algorithm	Curve	Values
EdDSA	RESERVED	0
EdDSA	EdDSA25519	1 [RFC8032]
EdDSA	EdDSA25519ph	2 [RFC8032]
EdDSA	EdDSA448	3 [RFC8032]
EdDSA	EdDSA448ph	4 [RFC8032]

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:

HIT Suite	Four-bit ID	Eight-bit encoding	
RESERVED	0	0x00	
EdDSA/cSHAKE128	5	0x50	(RECOMMENDED)

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.

Index	Hash function	HMAC	Signature algorithm family	Description
5	cSHAKE128	KMAC128	EdDSA	EdDSA HI hashed with cSHAKE128, output is 96 bits

Table 1: HIT Suites

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

DRIP Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 June 2021

A. Wiethuechter
S. Card
AX Enterprize, LLC
R. Moskowitz
HTT Consulting

17 December 2020

DRIP Authentication Formats
draft-wiethuechter-drip-auth-06

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.

Table of Contents

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

```
Page 0:
 0                   1                   2                   3
 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
+---------------+-----------------------------------------------+
|  Auth Header  |                                               |
+---------------+  ASTM Authentication Headers  +---------------+
|                                               |               |
+-----------------------------------------------+               |
|                                                               |
|                                                               |
|                                                               |
|                Authentication Data / Signature                |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+

Page 1 - 4:
 0                   1                   2                   3
 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
+---------------+-----------------------------------------------+
|  Auth Header  |                                               |
+---------------+                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                Authentication Data / Signature                |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+

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

```
Page 0:
 0                   1                   2                   3
 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
+---------------+-----------------------------------------------+
|  Auth Header  |                                               |
+---------------+  ASTM Authentication Headers  +---------------+
|                                               |  DRIP Header  |
+-----------------------------------------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                   DRIP Authentication Data                    |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+

Page 1 - Page N-1:
 0                   1                   2                   3
 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
+---------------+-----------------------------------------------+
|  Auth Header  |                                               |
+---------------+                                               |
|                                                               |
```

```
      |                                                               |
      |                                                               |
      |                   DRIP Authentication Data                    |
      |                                                               |
      |                                                               |
      |                                                               |
      |                                                               |
      |                                                               |
      +---------------------------------------------------------------+

      Page N:
       0                   1                   2                   3
       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
      +---------------+-----------------------------------------------+
      |  Auth Header  |                                               |
      +---------------+                                               |
      |                                                               |
      |                                                               |
      |                                                               |
      |                   Forward Error Correction                    |
      |                                                               |
      |                                                               |
      |                                                               |
      |                                                               |
      |                                                               |
      +---------------------------------------------------------------+

      DRIP Header (1 byte):
             7     6     5     4     3     2     1     0
          +-----+-----+-----+-----+-----+-----+-----+-----+
          | FEC |               DRIP AuthType             |
          +-----+-----+-----+-----+-----+-----+-----+-----+

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

          DRIP AuthType (7 bits):
              DRIP AuthType                        Values
              -------------                        ------
              0 Wrapped ASTM Message(s)            0
              1 Wrapped ASTM Message(s)            1
              2 Wrapped ASTM Message(s)            2
              3 Wrapped ASTM Message(s)            3
              4 Wrapped ASTM Message(s)            4
              5 Wrapped ASTM Message(s)            5
              8 Byte Manifest                      6
              4 Byte Manifest                      7
```

Reserved (Wrapped Messages)	8-15
Certificate: Registry on Aircraft	16
Reserved (Certificates)	17-31
Private Use	32-63
Reserved	64-111
Experimental Use	112-127

DRIP Authentication Data (200 bytes):
DRIP Authentication data. 0 to 200 bytes.

Forward Error Correction (23 bytes):
Optional and signaled using DRIP Header. Always last Authentication page.

Figure 2: DRIP General Frame Format

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)
```

Figure 3: DRIP Header Bitmasks

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).

```
  0                   1                   2                   3
  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
 +---------------+---------------+---------------+---------------+
 |                                                               |
 |                        UA Hierarchical                        |
 |                       Host Identity Tag                       |
 |                                                               |
 +---------------+---------------+---------------+---------------+
 |                        Trust Timestamp                        |
 +---------------+---------------+---------------+---------------+
 |                                                               |
 .                                                               .
 .                      Authentication Data                      .
 .                                                               .
 |                                                               |
 +---------------+---------------+---------------+---------------+
 |                                                               |
 |                                                               |
 |                                                               |
 |                                                               |
 |                                                               |
 |                           Signature                           |
 |                                                               |
 |                                                               |
 |                                                               |
 |                                                               |
```

```
      |                                                               |
      |                                                               |
      |                                                               |
      +---------------+---------------+---------------+---------------+
```

UA Hierarchial 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

```
 0                   1                   2                   3
 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
+---------------+---------------+---------------+---------------+
|                   Hash of Previous Manifest                   |
|                                                               |
+---------------+---------------+---------------+---------------+
|                    Hash of Current Manifest                   |
|                                                               |
+---------------+---------------+---------------+---------------+
|                         Message Hash 1                        |
|                                                               |
+---------------+---------------+---------------+---------------+
|                         Message Hash 2                        |
|                                                               |
+---------------+---------------+---------------+---------------+
.                                                               .
.                                                               .
.                                                               .
+---------------+---------------+---------------+---------------+
|                        Message Hash 12                        |
|                                                               |
+---------------+---------------+---------------+---------------+

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

```
 0                   1                   2                   3
 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
+---------------+---------------+---------------+---------------+
|                   Hash of Previous Manifest                   |
+---------------+---------------+---------------+---------------+
|                    Hash of Current Manifest                   |
+---------------+---------------+---------------+---------------+
|                         Message Hash 1                        |
+---------------+---------------+---------------+---------------+
|                         Message Hash 2                        |
+---------------+---------------+---------------+---------------+
.                                                               .
.                                                               .
.                                                               .
+---------------+---------------+---------------+---------------+
|                         Message Hash 27                       |
+---------------+---------------+---------------+---------------+

DRIP Header:
    With FEC: 0x86 [132] (RECOMMENDED)
    Without FEC: 0x06 [6]

Hash of Previous Manifest: (4 bytes)
    A hash of the previously sent Authentication message.

Hash of Current Manifest: (4 bytes)
    A hash of the current Authentication message.

Message Hash: (4 bytes)
    A hash of a previously sent message. 27 max.
```

Figure 6: 4 Byte Manifest

4.2.3.2.4. Pseudo-Blockchain Hashes

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 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).

```
    0                   1                   2                   3
    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
   +---------------+---------------+---------------+---------------+
   |                                                               |
   .                                                               .
   .                       Attestation Data                        .
   .                                                               .
   |                                                               |
   +---------------+---------------+---------------+---------------+
   |                     Expiration Timestamp                      |
   +---------------+---------------+---------------+---------------+
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                           Signature                           |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------+---------------+---------------+---------------+

   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 is 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

[F3411-19] "Standard Specification for Remote ID and Tracking", February 2020.

[NIST.SP.800-185] Kelsey, J., Change, S., and R. Perlner, "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash", DOI 10.6028/nist.sp.800-185, NIST Special Publication SP 800-185, December 2016, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-185.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

[drip-requirements] Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-06, 1 November 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-reqs-06.txt>.

[drip-rid] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-uas-rid-01, 9 September 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-uas-rid-01.txt>.

[identity-claims] Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Identity Claims", Work in Progress, Internet-Draft, draft-wiethuechter-drip-identity-claims-03, 2 November 2020, <http://www.ietf.org/internet-drafts/draft-wiethuechter-drip-identity-claims-03.txt>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

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