

drip
Internet-Draft
Intended status: Informational
Expires: June 17, 2021

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao (Editor)
Tencent
A. Gurtov
Linkoeping University
December 14, 2020

Drone Remote Identification Protocol (DRIP) Architecture
draft-ietf-drip-arch-06

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

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 June 17, 2021.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

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

Table of Contents

1.	Introduction	3
1.1.	Overview UAS Remote ID (RID) and RID Standardization	3
1.2.	Overview of Types of UAS Remote ID	4
1.2.1.	Network RID	4
1.2.2.	Broadcast RID	5
1.3.	Overview of USS Interoperability	5
1.4.	Overview of DRIP Architecture	6
2.	Conventions	8
3.	Definitions and Abbreviations	8
3.1.	Additional Definitions	8
3.2.	Abbreviations	8
4.	HHIT for UAS Remote ID	9
4.1.	HIT as a Trustworthy Remote ID	9
4.2.	HHIT for Remote ID Registration and Lookup	10
4.3.	HHIT for Remote ID Encryption	10
5.	DRIP RID Entities (WAS Entities and their interfaces)	10
5.1.	Private Information Registry	11
5.1.1.	Background	11
5.1.2.	Proposed Approach	11
5.2.	Public Information Registry	12
5.2.1.	Background	12
5.2.2.	Proposed Approach	12
5.3.	CS-RID concept	12
5.3.1.	Proposed optional CS-RID SDSP	13
5.3.2.	Proposed optional CS-RID Finder	13
6.	UAS Remote Identifiers	13
6.1.	Background	13
6.2.	Proposed Approach	14
7.	DRIP Transactions enabling Trustworthy	15
8.	Privacy for Broadcast PII	15
9.	IANA Considerations	16
10.	Security Considerations	16
11.	Acknowledgements	17
12.	References	17
12.1.	Normative References	17
12.2.	Informative References	17
Appendix A.	Overview of Unmanned Aircraft Systems (UAS) Traffic	19
A.1.	Operation Concept	19
A.2.	UAS Service Supplier (USS)	20
A.3.	UTM Use Cases for UAS Operations	20

A.4. Automatic Dependent Surveillance Broadcast (ADS-B) . . . 21
 Authors' Addresses 21

1. Introduction

This document describes a natural Internet and MAC-layer broadcast-based architecture for Unmanned Aircraft System Remote Identification and tracking (UAS RID), 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. Network RID

A RID data dictionary and data flow for Network RID are defined in [F3411-19]. This 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 this information to Network Remote ID Display Providers (Net-RID DP). It is the Net-RID DP that respond to queries from Network Remote ID clients (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 1 below:

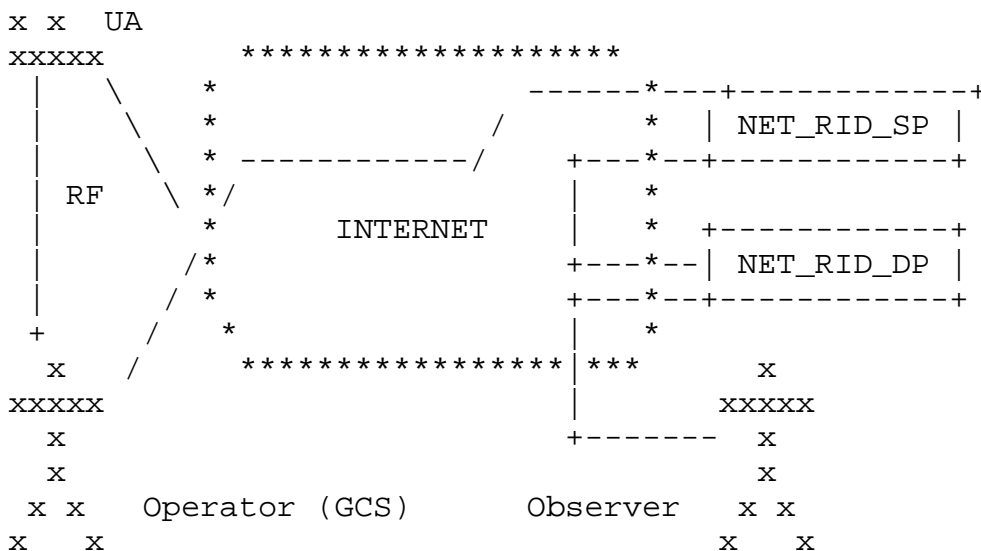


Figure 1

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.

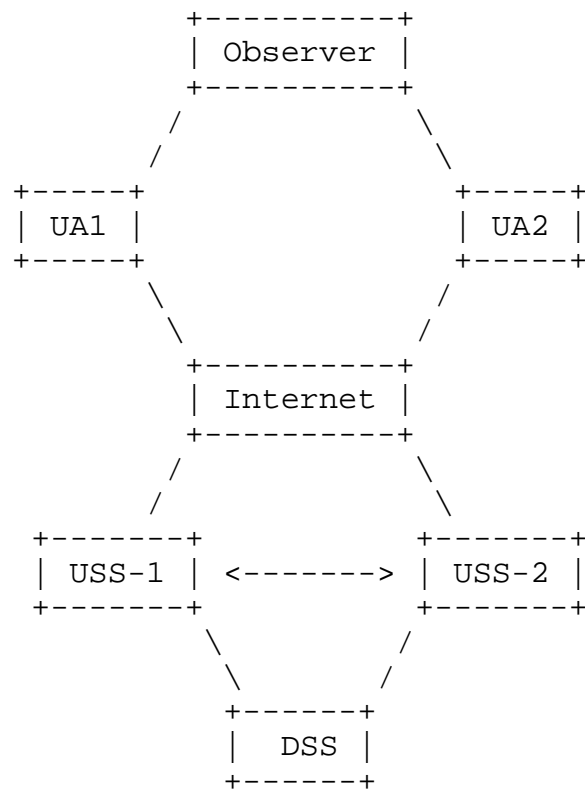


Figure 3

1.4. Overview of DRIP Architecture

The requirements document 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.

- o Mechanisms to leverage Domain Name System (DNS: [RFC1034]) and Extensible Provisioning Protocol (EPP [RFC5731]) technology to provide for private (Section 5.1) and public (Section 5.2) Information Registry.
- o Trustworthy Remote ID and trust in RID messages Section 6
- o Privacy in RID messages (PII protection) Section 8

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

- o UA -> Ground communications including Broadcast RID
- o Broadcast RID 'harvesting' and secure forwarding into the UTM
- o Secure UAS -> Net-RID SP communications
- o 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

Editor's Note: to be updated.

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

3.2. Abbreviations

Editor's Note: to be updated.

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

4. HHIT for UAS Remote ID

This section describes 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. HIT as a Trustworthy 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.

4.2. 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 key 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 original proposal for HITs included a registration hierarchy scheme. This was dropped during HIP development for lack of a use case. No similar mechanism is possible within CGAs. It is a rather straightforward design update to HITs to Hierarchical HITs (HHITs) to meet the UAS Remote ID use case.

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]).

4.3. 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 RID Entities (WAS Entities and their interfaces)

Editor: This section describes the DRIP RID ecosystem such as RID design philosophy, PII registration, Still not sure this is a good title since here mainly talks about register, maybe use this section focus on HHIT RID registration?? I also have suggestion to move the CS-RID to a separated section

Any DRIP solutions for UAS RID must fit into the UTM (or U-space) system. This implies interaction with entities including UA, GCS, USS, Net-RID SP, Net-RID DP, Observers, Operators, Pilots In Command, Remote Pilots, possibly SDSP, etc. The only additional entities introduced in this document are registries, required but not specified by the regulations and [RFC7401], and optionally CS-RID SDSP and Finder nodes.

UAS registries hold both public and private UAS information. The public information is primarily pointers to the repositories of, and keys for looking up, the private information. 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.

Editor's note: what are differences & relationships among public & private registries, DP, SP, USS

5.1. Private Information Registry

5.1.1. Background

The private information required for UAS RID is similar to that required for Internet domain name registration. Thus 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.

5.1.2. Proposed Approach

A DRIP UAS ID 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).

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].

5.2. Public Information Registry

5.2.1. Background

The public information required to be made available by UAS RID is transmitted as cleartext to local observers in Broadcast RID and is served to a client by a Net-RID DP in Network RID. Therefore, while IETF can offer e.g. [RFC6280] as one way to implement Network RID, the only public information required to support essential DRIP functions for UAS RID is that required to look up Internet domain hosts, services, etc.

5.2.2. Proposed Approach

A DRIP public information registry MUST be a standard DNS server, 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].

5.3. CS-RID concept

Editor's Note: if CS-RID is optional, may be added in separately section stating optional features Maybe add the CS into architecture diagram

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 considering Network RID also. 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. Such gateways could be pre-positioned (e.g. around airports and other sensitive areas) and/or crowdsourced (as nothing more than a smartphone with a suitable app is needed). As Broadcast RID media have limited range, gateways receiving messages claiming locations far from the gateway can alert authorities or a SDSP to the failed sanity check possibly indicating intent to deceive. Surveillance SDSPs can use messages with precise date/time/position stamps from the gateways to multilaterate UA location, independent of

the locations claimed in the messages, which are entirely operator self-reported in UAS RID and UTM. 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. CS-RID would be an option, beyond baseline DRIP functionality; if implemented, it adds two more entity types.

5.3.1. Proposed optional 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.

5.3.2. Proposed optional CS-RID Finder

A CS-RID Finder 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. A CS-RID Finder must implement, integrate, or accept outputs from, a Broadcast RID receiver. A CS-RID Finder MUST NOT interface directly with a GCS, Net-RID SP, Net-RID DP or Network RID client.

6. UAS Remote Identifiers

6.1. Background

A DRIP UA 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.

Within the limitations of Broadcast RID, this is extremely challenging as:

- o An RID can at most be 20 characters
- o The ASTM Basic RID message (the message containing the RID) is 25 characters; only 3 characters are currently unused

- o The ASTM Authentication message, with some changes from [F3411-19] can carry 224 bytes of payload.

Standard approaches like X.509 and PKI will not fit these constraints, even using the new EdDSA algorithm. An example of a technology that will fit within these limitations is an enhancement of the Host Identity Tag (HIT) of HIPv2 [RFC7401] introducing hierarchy as defined in HHIT [I-D.ietf-drip-rid]; using Hierarchical HITs 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.

6.2. Proposed Approach

A DRIP UAS ID MUST be a HHIT. It SHOULD be self-generated by the UAS (either UA or GCS) and MUST be registered with the Private Information Registry 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.

7. DRIP Transactions enabling Trustworthy

Each Operator MUST generate a Host Identity of the Operator (HIo) and derived Hierarchical HIT of the Operator (HHITo), register them with a Private Information Registry along with whatever Operator data (inc. PII) is required by the cognizant CAA and the registry, and obtain a Certificate from the Registry on the Operator (Cro) signed with the Host Identity of the Registry private key (HIr(priv)) proving such registration.

To add an 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

Editor's note: move this to a subsection of Operator Privacy?

Broadcast RID messages may contain PII. This may be information about the UA such as its destination or Operator information such as GCS location. There is no absolute "right" in hiding PII, as there will be times (e.g., disasters) and places (buffer zones around

airports and sensitive facilities) where policy may mandate all information be sent as cleartext. Otherwise, the modern general position (consistent with, e.g., the EU General Data Protection Regulation) is to hide PII unless otherwise instructed. While some have argued that a system like that of automobile registration plates should suffice for UAS, others have argued persuasively that each generation of new identifiers should take advantage of advancing technology to protect privacy, to the extent compatible with the transparency needed to protect safety.

A viable architecture for PII protection would be symmetric encryption of the PII using a key known to the UAS and a USS service. An authorized Observer may send the encrypted PII along with the Remote ID (to their UAS display service) to get the plaintext. The authorized Observer may send the Remote ID (to their UAS display service) and receive the key to directly decrypt all PII content from the UA.

PII is 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 USS 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.

9. IANA Considerations

Editor's note: placeholder

10. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. A manufacturer that embeds a private key in an UA may have retained a copy. A manufacturer whose UA are configured by a closed source application on the GCS which communicates over the Internet with the factory may be sending a copy of a UA or GCS self-generated key back to the factory. Keys may be extracted from a GCS or UA; the RID sender of a small harmless UA (or the entire UA) could be carried by a larger dangerous UA as a "false flag." Compromise of a registry private key could do widespread harm. Key revocation procedures are as yet to be determined. These risks are in addition to those involving Operator key management practices.

11. 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.

12. References

12.1. Normative References

[I-D.ietf-drip-reqs]

Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", draft-ietf-drip-reqs-06 (work in progress), November 2020.

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

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

12.2. Informative References

[CTA2063A]

ANSI, "Small Unmanned Aerial Systems Serial Numbers", 2019.

[Delegated]

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

[F3411-19]

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", draft-ietf-drip-rid-04 (work in progress), November 2020.

[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>>.

[RFC6280]

Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, DOI 10.17487/RFC6280, July 2011, <<https://www.rfc-editor.org/info/rfc6280>>.

- [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
USA

Email: stu.card@axenterprize.com

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

Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
USA

Email: rgm@labs.htt-consult.com

Shuai Zhao
Tencent
2747 Park Blvd
Palo Alto 94588
USA

Email: shuai.zhao@ieee.org

Andrei Gurtov
Linköping University
IDA
Linköping SE-58183 Linköping
Sweden

Email: gurtov@acm.org