drip
Internet-Draft
Intended status: Informational
Expires: 6 May 2021

S. Card
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
S. Zhao (Editor)
Tencent
A. Gurtov
Linköping University
2 November 2020

Drone Remote Identification Protocol (DRIP) Architecture
draft-ietf-drip-arch-05

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 6 May 2021.

Table of Contents

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 sighted by FAA in its RID [NPRM] as "one potential means of compliance" to a Remote ID rule.

3GPP

3GPP provides UA service in the LTE network since release 15 in published technical specification [TS-36.777]. Start from its release 16, it completed the UAS RID requirement study in [TS-22.825] and proposed use cases in the mobile network and the services that can be offered based on RID and ongoing release 17 specification works on enhanced UAS service requirement and

provides the protocol and application architecture support which is applicable for both 4G and 5G network. ATIS's recent report [ATIS-I-0000074] proposes architecture approaches for the 3GPP network to support UAS and one of which is put RID in higher 3GPP protocol stack such as using ASTM remote ID [F3411-19].

1.2. Overview of Types of UAS Remote ID

1.2.1. Network RID

Network RID defines a RID data dictionary and data flow: from a UAS via unspecified means to a Network Remote ID Service Provider (Net-RID SP); from the Net-RID SP to an integrated, or over the Internet to a separate, Network Remote ID Display Provider (Net- RID DP); from the Net-RID DP via the Internet to Network Remote ID clients in response to their queries (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.

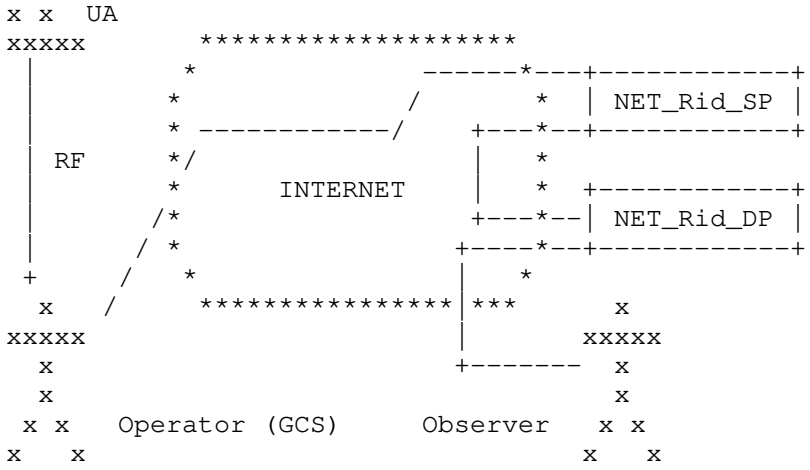


Figure 1

Via the direct Radio Frequency (RF) link between the UA and GCS: Command and Control (C2) flows from the GCS to the UA; for all but the simplest hobby aircraft, position and status flow from the UA to the GCS. Via the Internet, through three distinct segments, Network RID information flows from the UAS (comprising the UA and its GCS) to the Observer.

1.2.2. Broadcast RID

Broadcast RID defines a set of RID messages and how the UA transmits them locally directly one-way, over Bluetooth or Wi-Fi. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the locally directly received UAS ID as a key. Broadcast RID should be functionally usable in situations with no Internet connectivity.

The Broadcast RID is illustrated in Figure 2 below.

Editor's note: Is there a need to add interconnections between B-RID and N-RID in the drawing

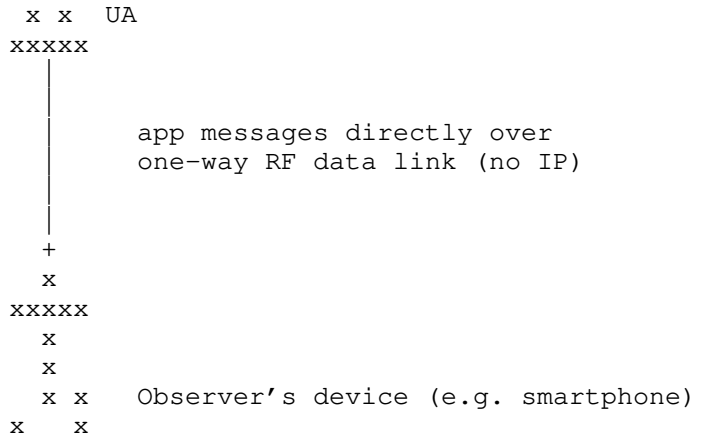


Figure 2

Editor's note: the following may more clarification:

* what Broadcast RID can do w/ & w/o Observer Internet connectivity

* How Broadcast RID transmits public info (obviating some registry lookups)

* how Network RID is "less constrained" than Broadcast RID

1.3. Overview of USS Interoperability

Editor's Note: Show how DRIP RID is an enabler of USS Interoperability Figure 3

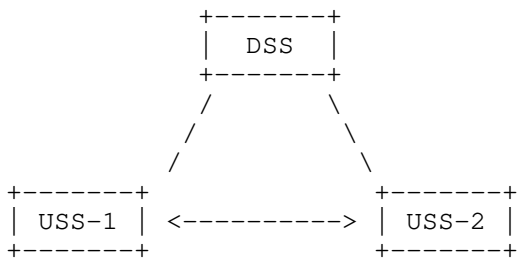


Figure 3

1.4. Overview of DRIP Archicture

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.

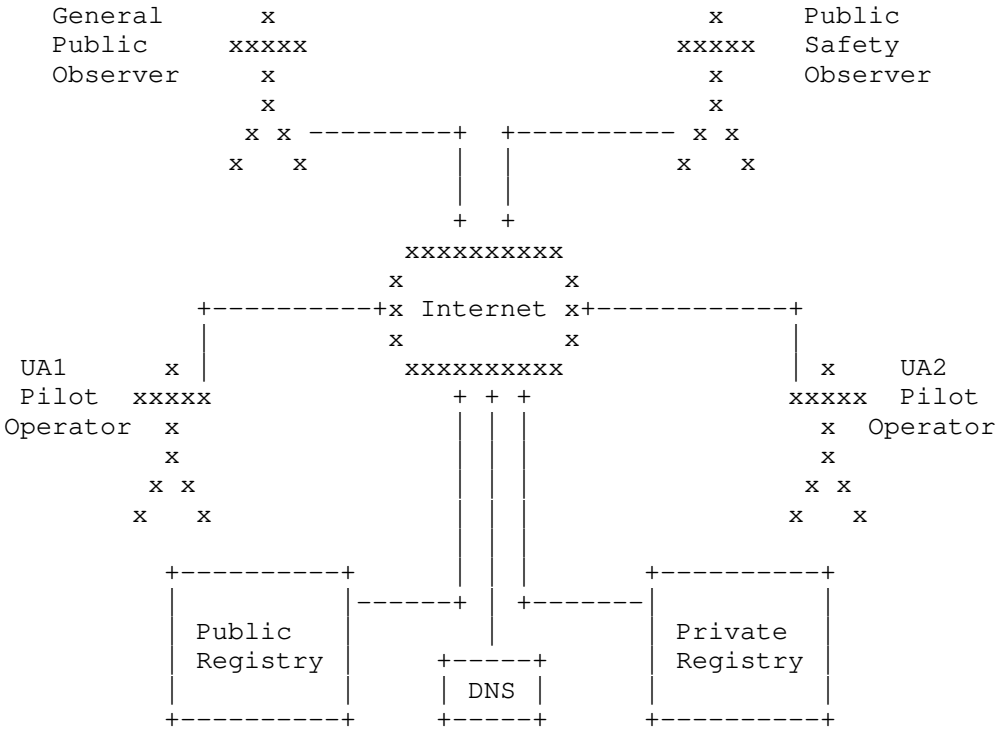


Figure 4

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

* add network RID and broadcast RID in the picture (since those are the focus points)

* 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 5.1) and public (Section 5.2) Information Registry.

* Trustworthy Remote ID and trust in RID messages Section 6

* Privacy in RID messages (PII protection) Section 8

  Eiditor's Note: 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

Editor's Note: to be updated.

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

> Editor's note: in order to make it self-contain, listing terms used in this draft should be okie, comments?

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 RID

Editor's note: I think we should explain HHIT designs for UAS RID first and give readers a direct imporession what this draft is offering. This is one of Daniel's comment, we shall focus on solutions, without repeating too much of details from a sepecifc draft.

This document 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.

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 (TBD; 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.

other pointers: (mostly list how HHIT satisfy the reqs-)

* Why DRIP RID should/MUST/May be a HHIT?

* HHIT RID format, metadate, and other useful info

* HHIT RID registar workflow

* HHIT Users (operator/USS/NETRID-SP?)

  - expand on different uses of & relationship between optional manufacturer-assigned HI & subsequent single-use HIs

* how security is guaranteed

  - call X.509 PKI not "standard" but "classical", describe it to justify why it won't work here

  - explain continuing role of some kind of CA even w/o X.509 PKI

> Editors' note: this is also one of the Michael's comment, we can address it here

* how DNS lookup may happen (Reverse DNS?)

* ....

5. DRIP RID Entities (WAS Entities and their interfaces)

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

* An RID can at most be 20 characters

* The ASTM Basic RID message (the message containing the RID) is 25 characters; only 3 characters are currently unused

* 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.moskowitz-hip-hierarchical-hit]; 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 ntoe: move this to a subsction 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", 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>.

[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

[ATIS-I-0000074]
ATIS, "Report on UAS in 3GPP", n.d., <https://access.atis.org/apps/group_public/download.php/48760/ATIS-I-0000074.pdf>.

[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-04, 1 November 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-rid-04.txt>.

[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, <http://www.ietf.org/internet-drafts/draft-maeurer-raw-ldacs-06.txt>.

[I-D.moskowitz-drip-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, <http://www.ietf.org/internet-drafts/draft-moskowitz-drip-crowd-sourced-rid-04.txt>.

[I-D.moskowitz-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-c2-01, 27 September 2020, <http://www.ietf.org/internet-drafts/draft-moskowitz-drip-secure-nrid-c2-01.txt>.

[I-D.moskowitz-hip-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>.

[I-D.moskowitz-hip-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>.

[I-D.moskowitz-hip-new-crypto]
Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-05, 26 July 2020, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-new-crypto-05.txt>.

[I-D.moskowitz-orchid-cshake]
Moskowitz, R., Card, S., and A. Wiethuechter, "Using cSHAKE in ORCHIDs", Work in Progress, Internet-Draft, draft-moskowitz-orchid-cshake-01, 21 May 2020, <http://www.ietf.org/internet-drafts/draft-moskowitz-orchid-cshake-01.txt>.

[I-D.wiethuechter-drip-auth]
Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-drip-auth-04, 21 September 2020, <http://www.ietf.org/internet-drafts/draft-wiethuechter-drip-auth-04.txt>.

[I-D.wiethuechter-drip-identity-claims]
Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Identity Claims", Work in Progress, Internet-Draft, draft-wiethuechter-drip-identity-claims-02, 26 October 2020, <http://www.ietf.org/internet-drafts/draft-wiethuechter-drip-identity-claims-02.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>.

[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>.

[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>.

[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>.

[TS-36.777] 3GPP, "UAV service in the LTE network", n.d., <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3231>.

[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 locaiton infomraiton, 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
na
Oak Park, MI, 48237
United States of America

Email: rgm@labs.htt-consult.com

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

Email: shuai.zhao@ieee.org

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping Linköping
Sweden

Email: gurtov@acm.org

DRIP
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2021

R. Moskowitz
HTT Consulting
S. Card
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

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 April 26, 2021.

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 Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 May 2021

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

2 November 2020

DRIP Identity Claims
draft-wiethuechter-drip-identity-claims-03

Abstract

This document describes the Identity Proofs (in the form of Claims, Certificates and Attestations) for use in various Drone Remote ID Protocols (DRIP) and the wider Unmanned Traffic Management (UTM) system.

Table of Contents

1. Introduction

DRIP Proofs are the backbone of trust in DRIP UAS RID, consisting of a chain of special certificates/attestations that results in a something useful in Broadcast RID. Some of the certificates are stored in and are generated by the Registries (defined in [hhit-registries]) and allow a user to confirm the trustworthiness of an Unmanned Aircraft (herein referred to as Aircraft) even in the scenario that the Observer is disconnected from the Internet.

1.1. Claims, Assertions, Attestations, and Certificates

The authors wish to make a clear distinction on exactly what these terms mean in the context of DRIP.

This is due 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 much discussion has been made around the terms being used.

1.1.1. 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.

1.1.2. 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 is a set of assertions. First that the identifier is unique and 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).

1.1.3. 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.

1.1.4. Certificates

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

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.

HDA: Hierarchial HIT Domain Authority. The 16 bit field identifying the HIT Domain Authority under a RAA.

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

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

3. DRIP Proofs

The DRIP Proofs is a set of custom structures to be used in the USS/UTM system. They are created during the provision of an Aircraft and are tied to the UAS ID (expected to be a HHIT, see [drip-rid] for details).

These structures when chained together can create a root of trust all the way back to the manufacturer itself during the initial production of a given Aircraft. The chain can also be used by authorized entities to trace an Aircraft through all owners and flights in the Aircraft's lifetime (something of interest to ICAO).

The rest of this section will define the formats of proofs in DRIP as forms of certificates and attestations and their common uses.

3.1. Certificate: X on X (Cxx Form)

The Cxx Form of DRIP Proofs is a self-signed certificate (by an entity known as 'X') staking an unverified claim on a HHIT/HI pairing until an expiration date/time.

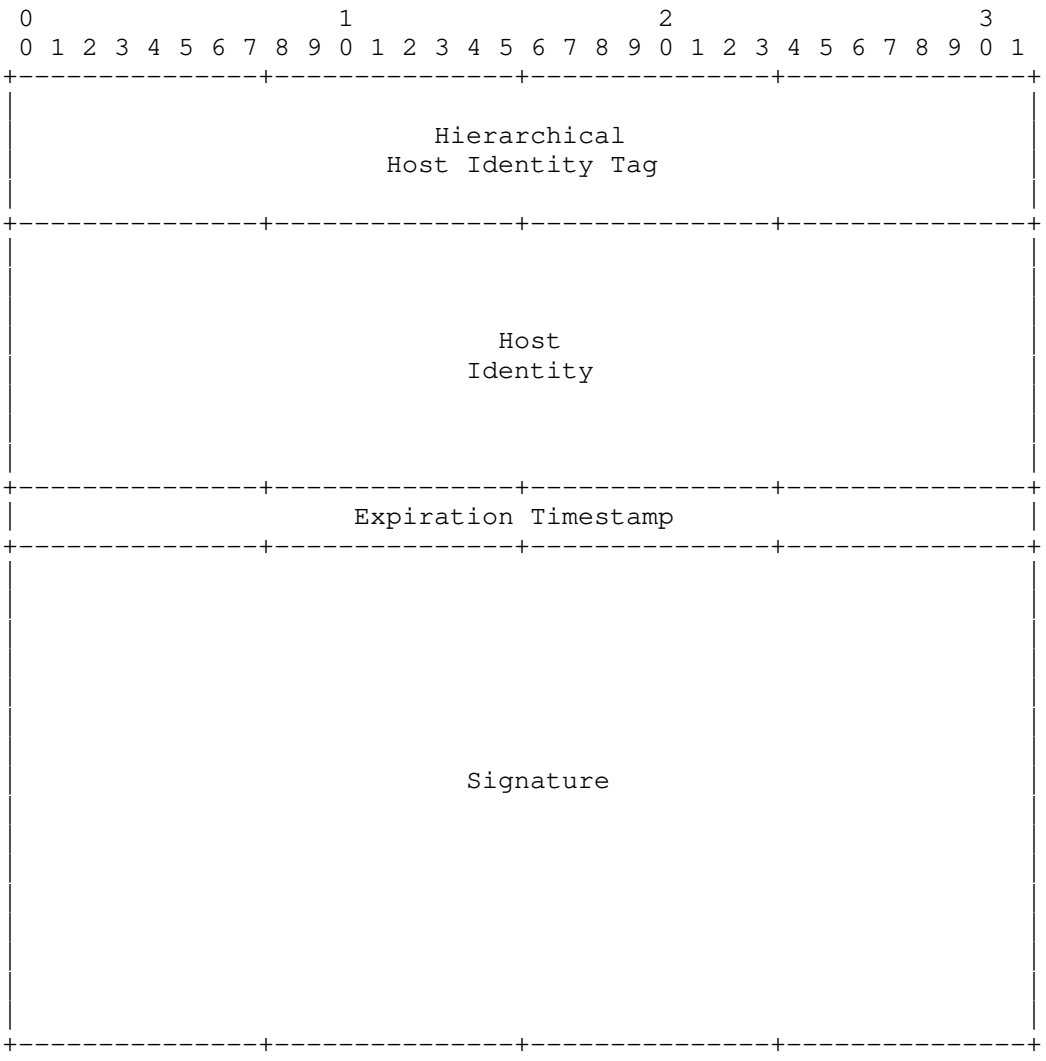


Figure 1: Certificate: X on X

Certificates of the Cxx Form are 116 bytes. The offset of the Expiration Timestamp SHOULD be of significant length (possibly years).

These are 5 (five) Cxx Certificates that can be created in a standard DRIP UAS RID system: Manufacturer on Manufacturer, RAA on RAA, HDA on HDA (Registry on Registry), Operator on Operator, and Aircraft on Aircraft. This is not an exhaustive list as any entity with the DRIP UAS system SHOULD have a Cxx for itself.

3.1.1. Certificate: X on X (Short Form)

A smaller version of Certificate: X on X exists where the Host Identity is removed allowing a claim to be made in 84 bytes.

Figure 2: Certificate: X on X (Short Form)

3.2. Attestation: X on Y (Axy Form)

This DRIP Proof is an attestation where Entity X asserts trust in the binding claimed by Entity Y (in Cyy) and signs this asserting with a timestamp and an expiration of when the binding is no longer asserted by Entity X.

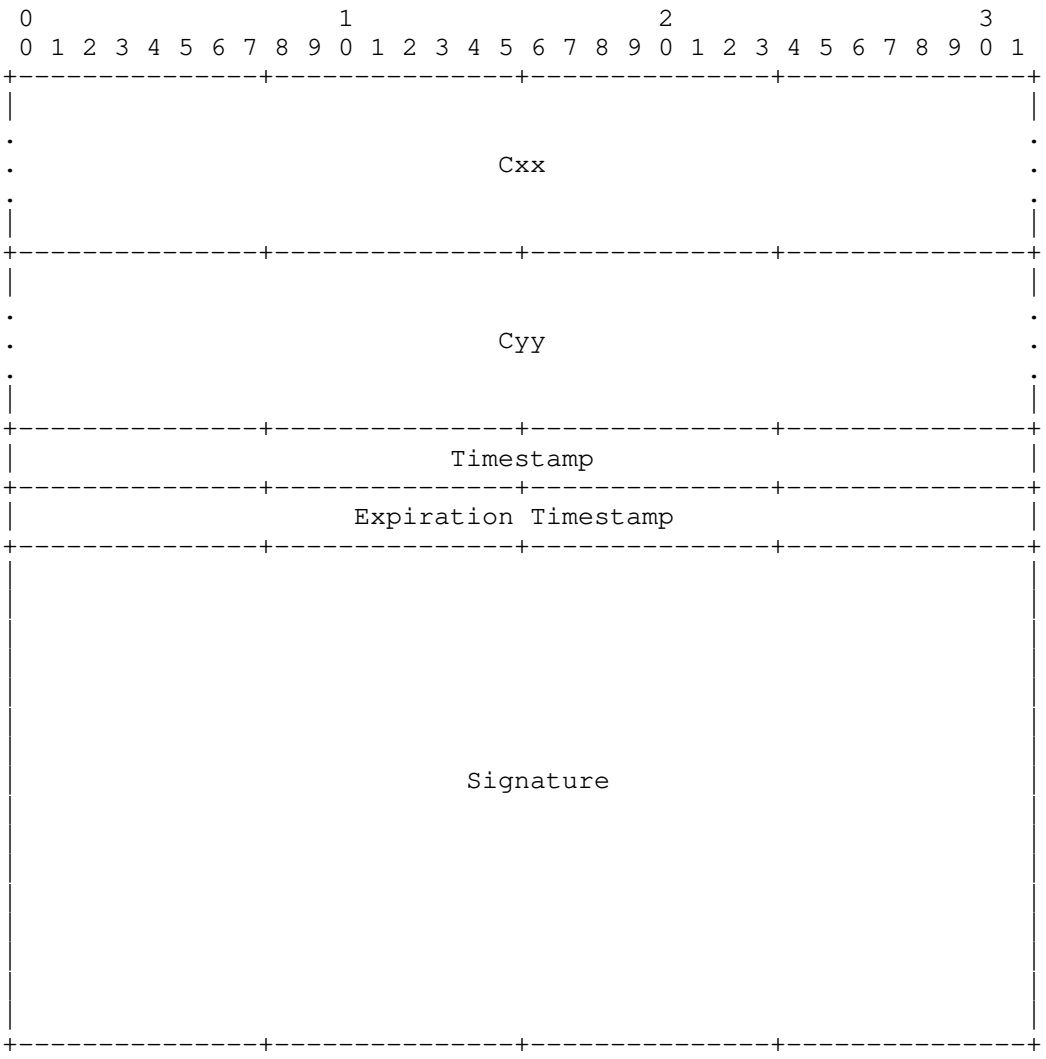


Figure 3: Attestation: X on Y

Axy Form wraps both self-signed certificates of the entities and is signed by Entity X. Two timestamps, one taken at the time of signing and one as an expiration time are used to set boundaries to the assertion. Care should be given to how far into the future the Expiration Timestamp is set, but is left up to system policy.

Most attestations of this form have a length of 304 bytes. Attestation: Registry on Operator on Aircraft is unique in that is 680 bytes long, binding of two Axy forms (in this specific case

Attestation: Registry on Operator with Attestation: Operator on Aircraft).

3.2.1. Attestation: X on Y (Short Form)

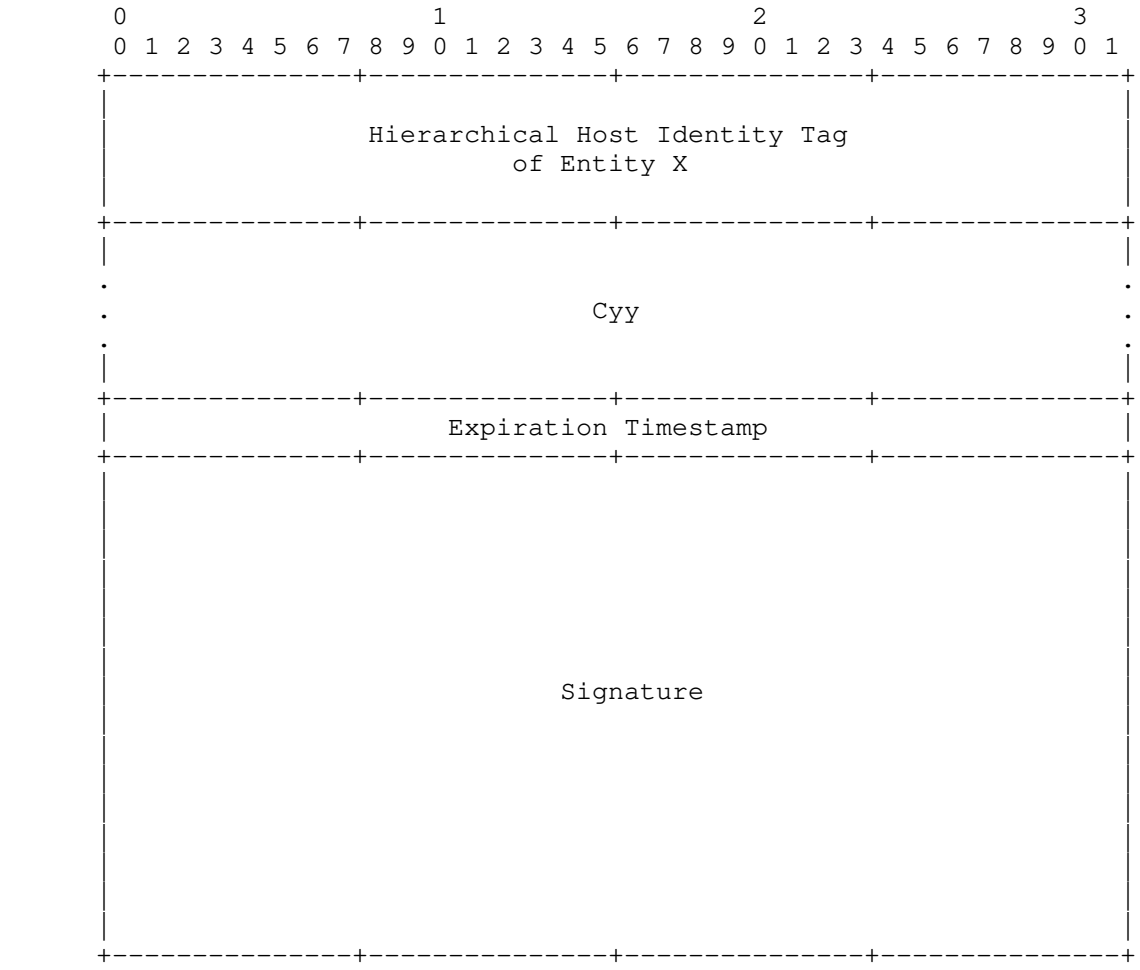


Figure 4: Attestation: X on Y (Short Form)

The short form of the Axy this attestation is 200 bytes long and is designed to fit inside the framing of the ASTM F3411 Authentication Message. The HHIT of Entity X is used in place of the full Cxx (see Section 5 for comments). The timestamp is removed and only an expiration timestamp is present.

During creation the Expiration Timestamp MUST be no later than the Expiration Timestamp found in Cyy.

3.2.2. Attestation: X on Y (Offline Form)

A special attestation that is the basis for a certificate finalized onboard the aircraft during flight. It is used in Broadcast RID to provide the trustworthiness of the Aircraft without the need of the Observer to be connected to the Internet.

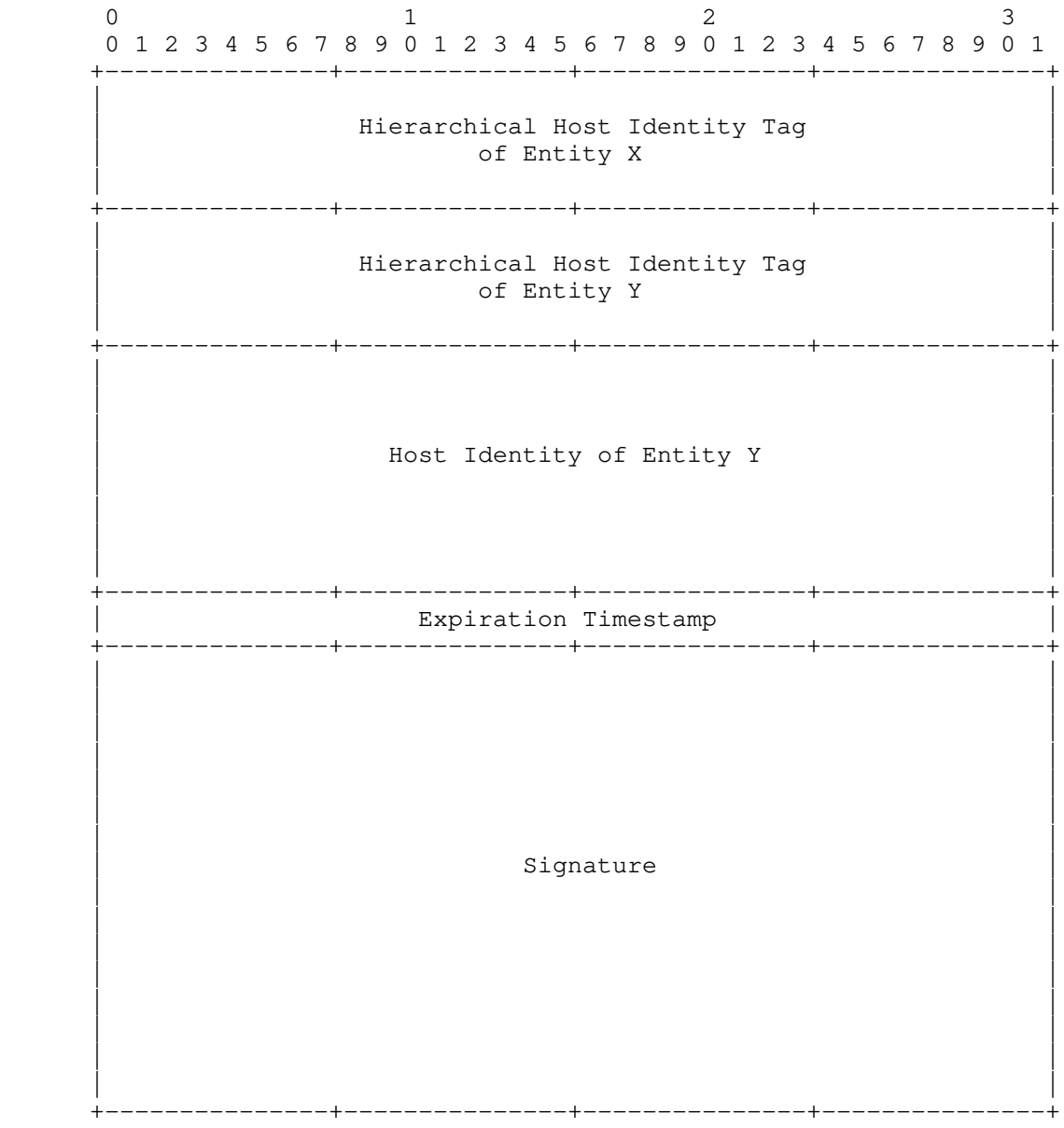


Figure 5: Attestation: X on Y (Offline Form)

The signature is generated using Entity X's keypair.

3.3. Timestamps

Timestamps MAY be the standard UNIX time or a protocol specific timestamp, to avoid programming complexities. For example [F3411-19] uses a 00:00:00 01/01/2019 offset. When a Expiration Timestamp is required a desired offset is added, setting the timestamp into the future. The amount of offset for specific timestamps is left to best practice.

3.4. Signatures

Signatures are ALWAYS taken over the preceding fields in the certificate/attestation. For DRIP the EdDSA25519 algorithm from [RFC8032] is used.

4. Provisioning

Under DRIP UAS RID a special provisioning procedure is required to properly generate and distribute the certificates and attestations to all parties in the USS/UTM ecosystem using DRIP RID.

Keypairs are expected to be generated on the device hardware it will be used on. Due to hardware limitations (see Section 5) and connectivity it is acceptable under DRIP RID to generate keypairs for the Aircraft on Operator devices and later securely inject them into the Aircraft (as defined in Section 4.5.2). The methods to securely inject and store keypair information in a "secure element" of the Aircraft is out of scope of this document.

4.1. HHIT Delegation

Under the FAA [NPRM], it is expecting that IDs for UAS are assigned by the UTM and are generally one-time use. The methods for this however are unspecified leaving two options.

1 The entity generates its own HHIT, discovering and using thr RAA and HDA for the target Registry. The method for discovering a Registry's RAA and HDA is out of scope here. This allows for the device to generate an HHIT to send to the Registry to be accepted (thus generating the required Host Identity Claim) or denied.

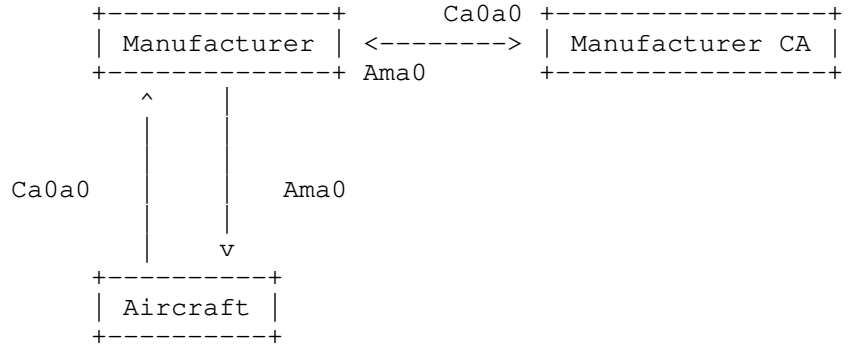
2 The entity sends to the Registry its HI for it to be hashed and result in the HHIT. The Registry would then either accept (returning the HHIT to the device) or deny this pairing.

In either case the Registry must decide on if the HI/HHIT pairing is valid. This in its simplest form is checking the current Registry for a collision on the HHIT.

Upon accepting a HI/HHIT pair the Registry MUST populate the required the DNS serving the HDA with the HIP RR and other relevant RR types (such as TXT and CERT). The Registry MUST also generate the appropriate Host Identity Claim for the given operation.

If the Registry denied the HI/HHIT pair, because there was a HHIT collision or any other reason, the Registry MUST signal back to the device being provisioned that a new HI needs to be generated.

4.2. Manufacturer



During the initial configuration and production at the factory the Aircraft MUST be configured to have a serial number. ASTM defines this to be an ANSI/CTA-2063A. Under DRIP a HHIT can be encoded as such to be able to convert back and forth between them. This is out of scope for this document.

Under DRIP the Manufacturer SHOULD be using HHITs and have their own keypair and Cxx (Certificate: Manufacturer on Manufacturer). (Ed. Note: some words on aircraft keypair and certs here?).

Certificate: Aircraft 0 on Aircraft 0 (Ca0a0) is extracted by the manufacturer and send to their Certificate Authority (CA) to be verified and added. A resulting certificate (Attestation: Manufacturer on Aircraft 0) SHOULD be a DRIP Attestation in the Axy Form - however this could be a X.509 certificate binding the serial number to the manufacturer.

4.3. Registry

TODO

DRIP UAS RID defines two levels of hierarchy maintained by the Registration Assigning Authority (RAA) and HHIT Domain Authority (HDA). The authors anticipate that an RAA is owned and operated by a

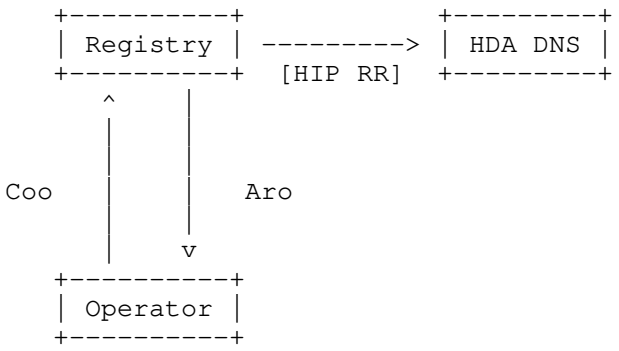
regional CAA (or a delegated party by an CAA in a specific airspace region) with HDAs being contracted out. As such a chain of trust for registries is required to ensure trustworthiness is not compromised. More information on the registries can be found in [hhit-registries].

Both the RAA and HDA generate their own keypairs and self-signed certificates (Certificate: RAA on RAA and Certificate: HDA on HDA respectively). The HDA sends to the RAA its self-signed certificate to be added into the RAA DNS.

The RAA confirms the certificate received is valid and that no HHIT collisions occur before added a HIP RR to its DNS for the new HDA. An Attestation: RAA on HDA is sent as a confirmation that provisioning was successful.

The HDA is now a valid "Registry" and uses its keypair and Certificate: HDA on HDA with all provisioning requests from downstream.

4.4. Operator



The Operator generates a keypair and HHIT as specified in DRIP UAS RID. A self-signed certificate (Certificate: Operator on Operator) is generated and sent to the desired Registry (HDA). Other relevant information and possibly personally identifiable information needed may also be required to be sent to the Registry (all over a secure channel - the method of which is out of scope for this document).

The Registry cross checks any personally identifiable information as required. Certificate: Operator on Operator is verified (both using the expiration timestamp and signature). The HHIT is searched in the Registries database to confirm that no collision occurs. A new attestation is generated (Attestation: Registry on Operator) and sent securely back to the Operator. Optionally the HHIT/HI pairing can be added to the Registries DNS in to form of a HIP Resource Record (RR).

Other RRs, such as CERT and TXT, may also be used to hold public information.

With the receipt of Attestation: Registry on Operator the provisioning of an Operator is complete.

4.5. Aircraft

4.5.1. Standard Provisioning

Under standard provisioning the Aircraft has its own connectivity to the Registry, the method which is out of scope for this document.

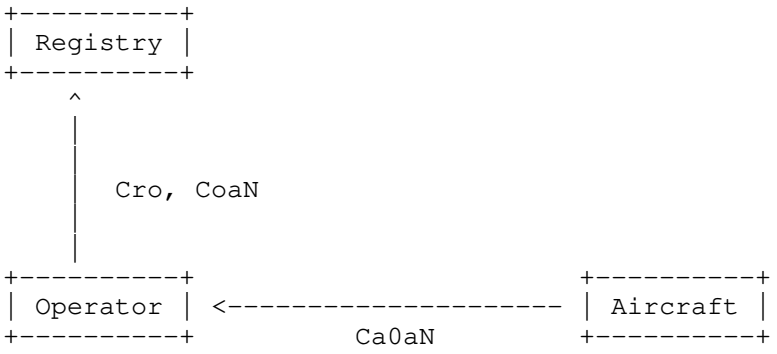


Figure 6: Standard Provision: Step 1

Through mechanisms not specified in this document the Aircraft should have methods to instruct the Aircrafts onboard systems to generate a keypair and certificate. This certificate is chained to the factory provisioned certificate (Certificate: Aircraft 0 on Aircraft 0). This new attestation (Attestation: Aircraft 0 on Aircraft N) is securely extracted by the Operator.

With Attestation: Aircraft 0 on Aircraft N the sub certificate (Certificate: Aircraft N on Aircraft N) is used by the Operator to generate Attestation: Operator on Aircraft N. This along with Attestation: Registry on Operator is sent to the Registry.

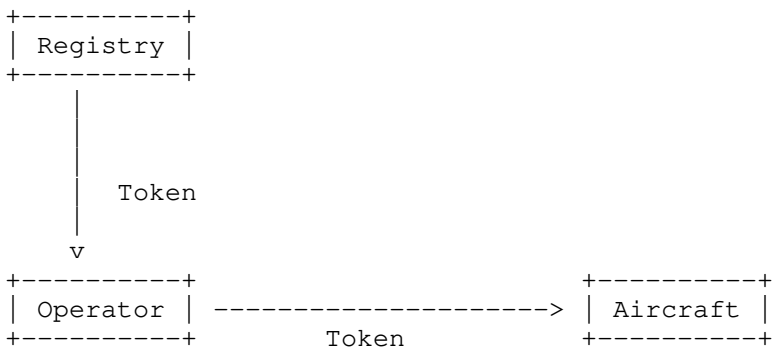


Figure 7: Standard Provision: Step 2

On the Registry, Attestation: Registry on Operator is verified and used as confirmation that the Operator is already registered. Attestation: Operator on Aircraft N also undergoes a validation check and used to generate a token to return to the Operator to continue provisioning.

Upon receipt of this token, the Operator injects it into the Aircraft and its used to form a secure connection to the Registry. The Aircraft then sends Attestation: Manufacturer on Aircraft 0 and Attestation: Aircraft 0 to Aircraft N.

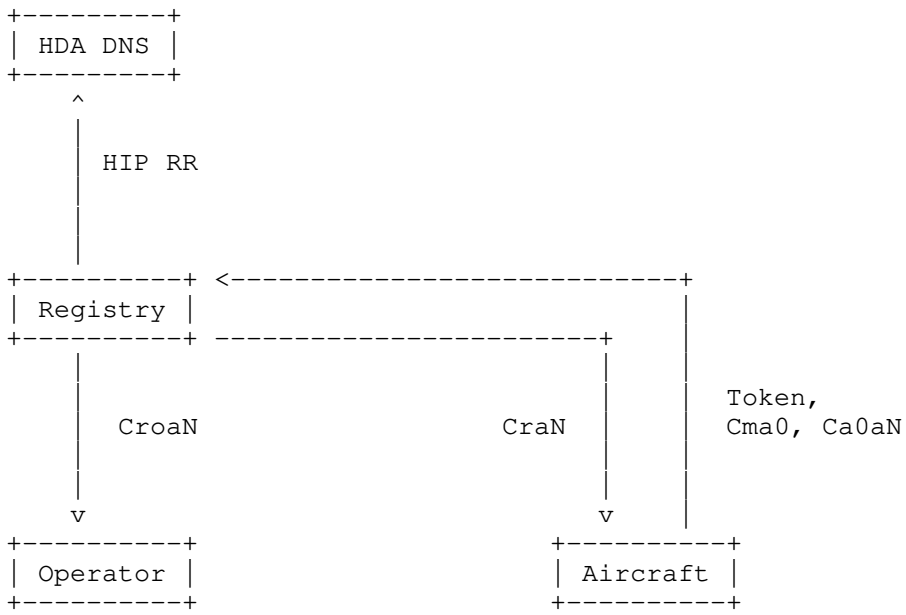


Figure 8: Standard Provision: Step 3

The Registry uses Attestation: Manufacturer on Aircraft 0 (with an external database if supported) to confirm the validity of the Aircraft. Attestation: Aircraft 0 on Aircraft N is correlated with Attestation: Operator on Aircraft N and Attestation: Manufacturer on Aircraft 0 to see the chain of ownership. The new HHIT tied to Aircraft N is then checked for collisions in the HDA. With the information the Registry generates two certificates: Attestation: Registry on Operator on Aircraft N and Attestation: Registry on Aircraft N (Offline Form). A HIP RR (and other RR types as needed) are generated and inserted into the HDA.

Attestation: Registry on Operator on Aircraft N is sent via a secure channel back to the Operator to be stored. Attestation: Registry on Aircraft N (Offline Form) is sent to the Aircraft to be used in Broadcast RID.

4.5.2. Operator Assisted Provisioning

This provisioning scheme is for when the Aircraft is unable to connect to the Registry itself or does not have the hardware required to generate keypairs and certificates.

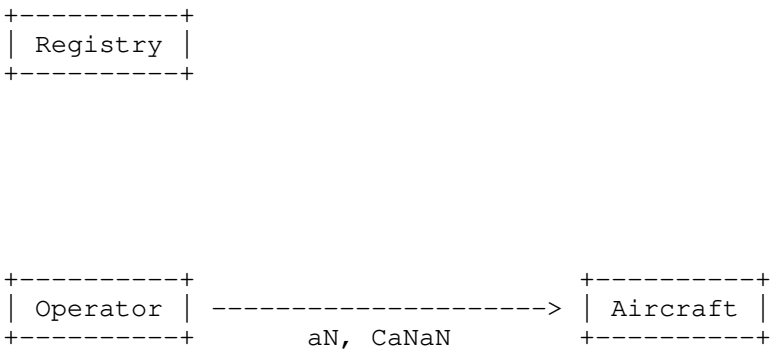


Figure 9: Operator Assisted Provision: Step 1

To start the Operator generates on behalf of the Aircraft a new keypair and Certificate: Aircraft N on Aircraft N. This keypair and certificate are injected into the Aircraft for it to generate Attestation: Aircraft 0 on Aircraft N. After injecting the keypair and certificate, the Operator MUST destroy all copies of the keypair.

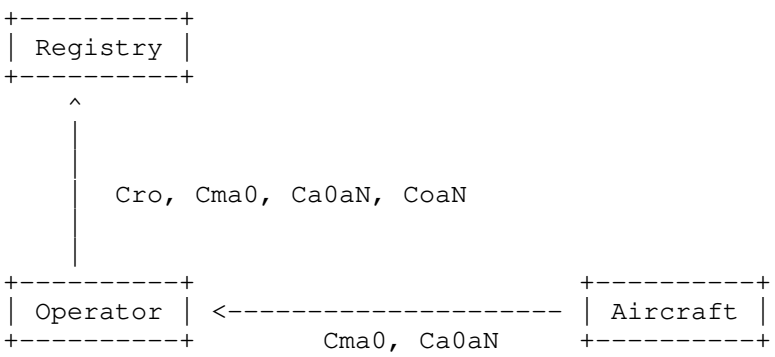


Figure 10: Operator Assisted Provision: Step 2

Attestation: Manufacturer on Aircraft 0 and Attestation: Aircraft 0 on Aircraft N is extracted by the Operator and the following data items are sent to the Registry; Attestation: Registry on Operator, Attestation: Manufacturer on Aircraft 0, Attestation: Aircraft 0 on Aircraft N, Attestation: Operator on Aircraft N.

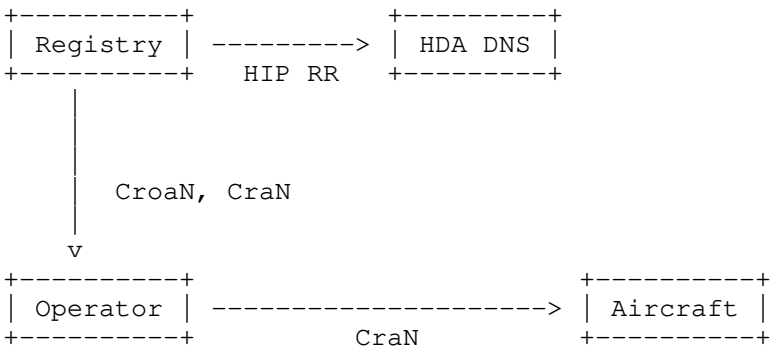


Figure 11: Operator Assisted Provision: Step 3

On the Registry validation checks are done on all attestations as per the previous sections. Once complete then the Registry checks for a HHIT collision, adding to the HDA if clear and generates Attestation: Registry on Operator on Aircraft N and Attestation: Registry on Aircraft N (Offline Form). Both are sent back to the Operator.

The Operator securely inject Attestation: Registry on Aircraft N (Offline Form) and securely stores Attestation: Registry on Operator on Aircraft N.

4.5.3. Initial Provisioning

A special form of provisioning is used when the Aircraft is first sold to an Operator. Instead of generating a new keypair, the built in keypair and certificate done by the Manufacturer is used to provision and register the aircraft to the owner.

For this either Standard or Operator Assisted methods can be used.

5. Security Considerations

A major consideration is the optimization done in Attestation: X on Y (Short Form) to get its length down to 200 bytes. The truncation of Certificate: HDA on HDA down to just its HHIT is one that could be used against the system to act as a false Registry. For this to occur an attacker would need to find a hash collision on that Registry HHIT and then manage to spoof all of DNS being used in the system.

The authors believe that the probability of such an attack is low when Registry operators are using best practices in security. If such an attack can occur (especially in the time frame of "one-time use IDs") then there are more serious issues present in the system.

6. References

6.1. Normative References

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

[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>.

6.2. 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>.

[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>.

[NPRM] "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019.

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