drip Working Group A. Wiethuechter

Internet-Draft S. Card

Intended status: Standards Track AX Enterprize, LLC

Expires: 26 August 2021 R. Moskowitz

HTT Consulting

22 February 2021

DRIP Registries

draft-wiethuechter-drip-registries-00

Abstract

This document focus on DRIP-related registries and the associated registration procedures that are required for Unmanned Aircraft System Remote Identification and tracking (UAS RID) purposes.

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 26 August 2021.

Copyright Notice

Copyright (c) 2021 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.

Wiethuechter, et al. Expires 26 August 2021 [Page 1]

Internet-Draft registries February 2021

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2

2. Terminology . . . . . . . . . . . . . . . . . . . . . . . . . 2

2.1. Required Terminology . . . . . . . . . . . . . . . . . . 2

2.2. Definitions . . . . . . . . . . . . . . . . . . . . . . . 2

3. Provisioning . . . . . . . . . . . . . . . . . . . . . . . . 3

3.1. Overview of Transactions . . . . . . . . . . . . . . . . 3

3.2. HHIT Delegation . . . . . . . . . . . . . . . . . . . . . 4

3.3. Manufacturer . . . . . . . . . . . . . . . . . . . . . . 4

3.4. Registry . . . . . . . . . . . . . . . . . . . . . . . . 5

3.5. Operator . . . . . . . . . . . . . . . . . . . . . . . . 6

3.6. Aircraft . . . . . . . . . . . . . . . . . . . . . . . . 6

3.6.1. Standard Provisioning . . . . . . . . . . . . . . . . 7

3.6.2. Operator Assisted Provisioning . . . . . . . . . . . 9

3.6.3. Initial Provisioning . . . . . . . . . . . . . . . . 10

4. Security Considerations . . . . . . . . . . . . . . . . . . . 10

5. References . . . . . . . . . . . . . . . . . . . . . . . . . 10

5.1. Normative References . . . . . . . . . . . . . . . . . . 10

5.2. Informative References . . . . . . . . . . . . . . . . . 11

Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 11

1. Introduction

TODO

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

This document makes use of the terms defined in [drip-requirements]. The following additional terms are defined in this document:

HDA: Hierarchial Host Identity Tags (HIT) Domain Authority. The 16 bit field identifying

the HIT Domain Authority under a RAA.

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

RAA: Registered Assigning Authority. The 16 bit field identifying

the Hierarchical HIT Assigning Authority.

Wiethuechter, et al. Expires 26 August 2021 [Page 2]

Internet-Draft registries February 2021

3. Provisioning

Under DRIP UAS RID, a 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 4) and

connectivity it is acceptable under DRIP RID to generate keypairs for

the UA on Operator devices and later securely inject them into

the UA (as defined in Section 3.6.2). The methods to securely

inject and store keypair information in a "secure element" of the

UA is out of scope of this document.

3.1. Overview of Transactions

Each Operator MUST generate a Host Identity of the Operator

(HIo) and derived Hierarchical HIT of the Operator (HHITo). These

are registered with a Private Information Registry along with

whatever Operator data (inc. PII) is required by the cognizant CAA

and the registry. In response, the Operator will obtain a

Certificate from the Registry, an Operator (Cro), signed with the

Host Identity of the Registry private key (HIr(priv)) proving such

registration.

An Operator may now add a UA. To do that, The Operator MUST:

\* Generate a Host Identity of the UA (HIa)

and derived Hierarchical HIT of the UA (HHITa)

\* Create a Certificate from the Operator on the UA (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 that Registry on the Operator and

Aircraft ("Croa") signed with the HIr(priv) proving such

Registration.

\* Obtain a Certificate from the Registry on the Aircraft (Cra)

signed with HIr(priv) proving UA registration in that specific

registry while preserving Operator’s privacy.

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

and Cra.

Wiethuechter, et al. Expires 26 August 2021 [Page 3]

Internet-Draft registries February 2021

\* An UA engaging in Broadcast RID MUST use HIa(priv) to sign Auth

Messages and MUST periodically broadcast Cra.

\* An UA 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.

3.2. HHIT Delegation

Under the FAA [NPRM], it is expected 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 the 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 whether the HI/HHIT pairing is

valid. This is in its simplest form about checking the current Registry

for a collision based upon the HHIT.

Upon accepting a HI/HHIT pair, the Registry MUST populate the required

the DNS records 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.

3.3. Manufacturer

Wiethuechter, et al. Expires 26 August 2021 [Page 4]

Internet-Draft registries February 2021

+--------------+ Ca0a0 +-----------------+

| Manufacturer | <--------> | Manufacturer CA |

+--------------+ Ama0 +-----------------+

^ |

| |

| |

Ca0a0 | | Ama0

| |

| v

+----------+

| Aircraft |

+----------+

During the initial configuration and production at the factory the

UA 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.

If DRIP mechanisms are used, 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.

3.4. 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.

Wiethuechter, et al. Expires 26 August 2021 [Page 5]

Internet-Draft registries February 2021

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.

3.5. Operator

+----------+ +---------+

| Registry | ---------> | HDA DNS |

+----------+ [HIP RR] +---------+

^ |

| |

| |

Coo | | Aro

| |

| v

+----------+

| 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.

3.6. Aircraft

Wiethuechter, et al. Expires 26 August 2021 [Page 6]

Internet-Draft registries February 2021

3.6.1. Typical Provisioning

Under standard provisioning the Aircraft has its own connectivity to

the Registry, the method which is out of scope for this document.

+----------+

| Registry |

+----------+

^

|

|

| Cro, CoaN

|

|

+----------+ +----------+

| Operator | <--------------------- | Aircraft |

+----------+ Ca0aN +----------+

Figure 1: 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.

+----------+

| Registry |

+----------+

|

|

|

| Token

|

v

+----------+ +----------+

| Operator | ---------------------> | Aircraft |

+----------+ Token +----------+

Figure 2: Standard Provision: Step 2

Wiethuechter, et al. Expires 26 August 2021 [Page 7]

Internet-Draft registries February 2021

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.

+---------+

| HDA DNS |

+---------+

^

|

| HIP RR

|

|

|

+----------+ <----------------------------+

| Registry | |

+----------+ ------------------------+ |

| | |

| | | Token,

| CroaN CraN | | Cma0, Ca0aN

| | |

| | |

v v |

+----------+ +----------+

| Operator | | Aircraft |

+----------+ +----------+

Figure 3: 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

Wiethuechter, et al. Expires 26 August 2021 [Page 8]

Internet-Draft registries February 2021

Aircraft N (Offline Form) is sent to the Aircraft to be used in

Broadcast RID.

3.6.2. 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.

+----------+

| Registry |

+----------+

+----------+ +----------+

| Operator | ---------------------> | Aircraft |

+----------+ aN, CaNaN +----------+

Figure 4: 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.

+----------+

| Registry |

+----------+

^

|

|

| Cro, Cma0, Ca0aN, CoaN

|

|

+----------+ +----------+

| Operator | <--------------------- | Aircraft |

+----------+ Cma0, Ca0aN +----------+

Figure 5: 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,

Wiethuechter, et al. Expires 26 August 2021 [Page 9]

Internet-Draft registries February 2021

Attestation: Manufacturer on Aircraft 0, Attestation: Aircraft 0 on

Aircraft N, Attestation: Operator on Aircraft N.

+----------+ +---------+

| Registry | ---------> | HDA DNS |

+----------+ HIP RR +---------+

|

|

|

| CroaN, CraN

|

v

+----------+ +----------+

| Operator | ---------------------> | Aircraft |

+----------+ CraN +----------+

Figure 6: 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.

3.6.3. 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.

4. Security Considerations

TODO

5. References

5.1. Normative References

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

February 2020.

Wiethuechter, et al. Expires 26 August 2021 [Page 10]

Internet-Draft registries February 2021

[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>.

5.2. 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

Wiethuechter, et al. Expires 26 August 2021 [Page 11]

Internet-Draft registries February 2021

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

Wiethuechter, et al. Expires 26 August 2021 [Page 12]