drip Working Group
Internet-Draft
Intended status: Standards Track
Expires: 29 April 2021

A. Wiethuechter
S. Card
AX Enterprize, LLC
R. Moskowitz
HTT Consulting
26 October 2020

DRIP Identity Claims
draft-wiethuechter-drip-identity-claims-02

Abstract

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

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 29 April 2021.

Table of Contents

1. Introduction

DRIP Certificates are the backbone of trust in DRIP UAS RID, consisting of a chain of special certificates that results in a compact certificate that is used in Broadcast RID. Some of the certificates are stored in and are generated by the Registries (defined in Section 4.3) 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. Use of the word Certificate

The certificates defined in the document were originally referred to as Host Identity Claims as early in the documents inception the authors felt that a distinction should have been drawn between certificates and what was being defined here.

This was 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/business platform for trusted identity management and was pursued in international bodies with links into treaty instruments.

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 (i.e. RAA + HDA).

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

3. DRIP Certificates

The DRIP Certificates is a set of custom certificates to be used in the USS/UTM system. They are created during the provision of an Aircraft and are tied to the UAS ID [drip-rid].

These certificates when chained together can create a chain of trust 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 (ICAO practice on manned aircraft).

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

3.1. Certificate: X on X (Cxx Form)

The Cxx Form of DRIP Certificates 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.

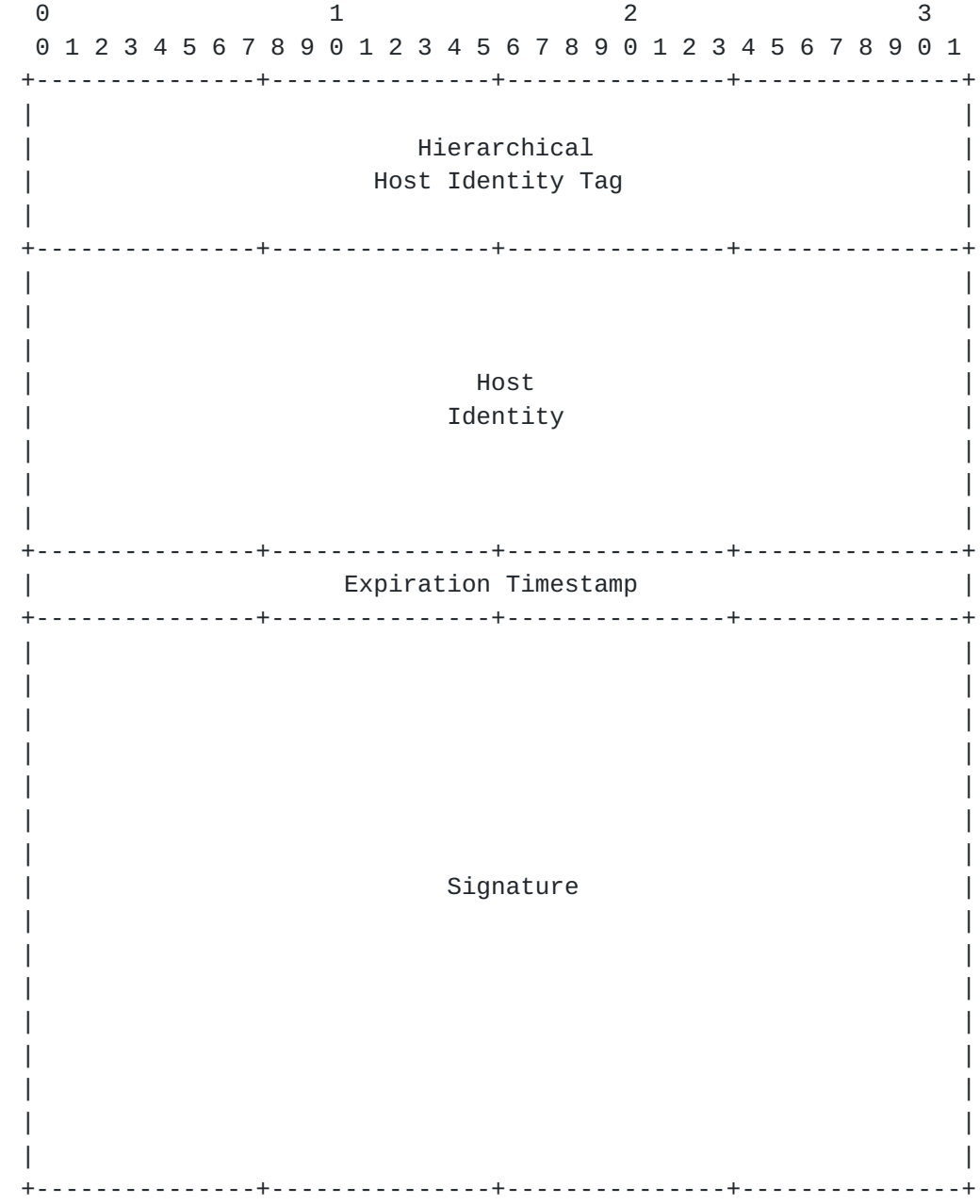


Figure 1: Certificate: X on X

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.

The Host Identity is expected to be looked up via [hhit-registries] when connected to the Internet. The smaller size of this certificate has the downside of not allowing for signature verification when Internet connectivity is unavailible to retreive the Host Identity.

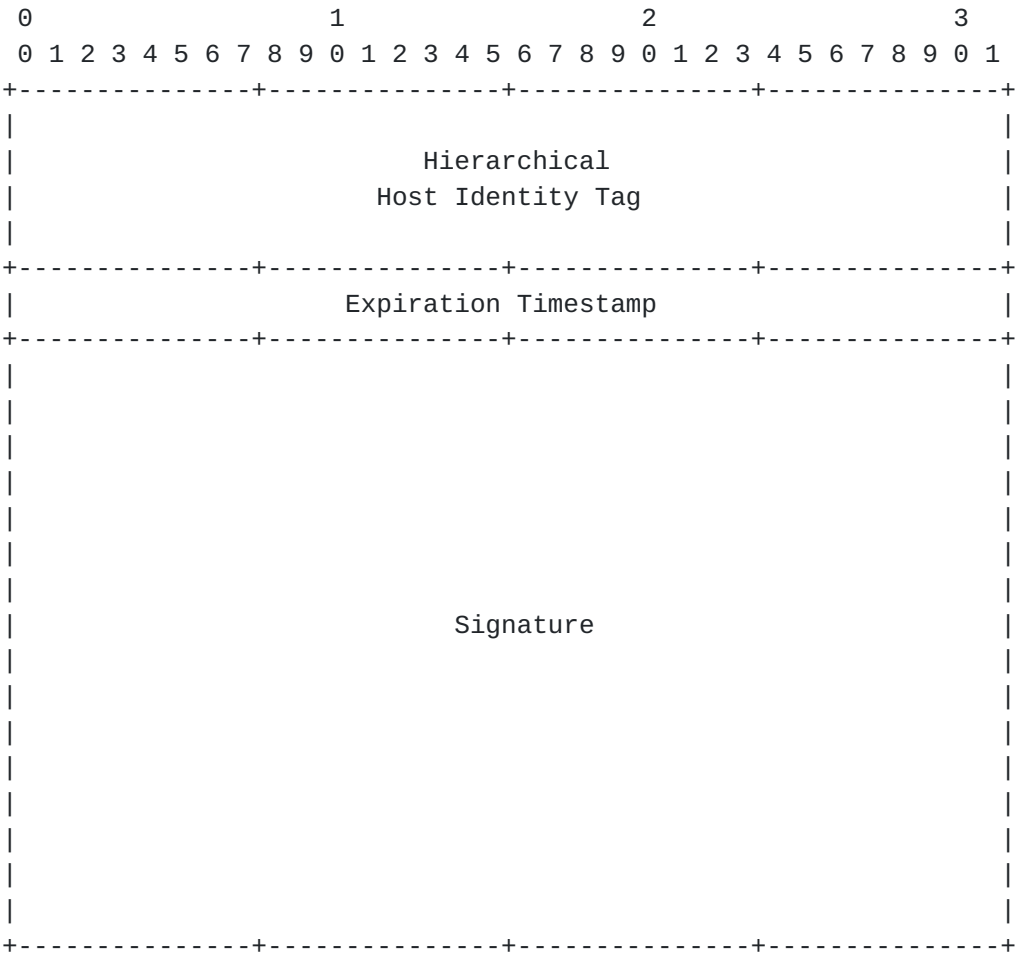


Figure 2: Certificate: X on X (Short Form)

3.2. Certificate: X on Y (Cxy Form)

The Cxy Form of DRIP Certificates is a certificate 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.

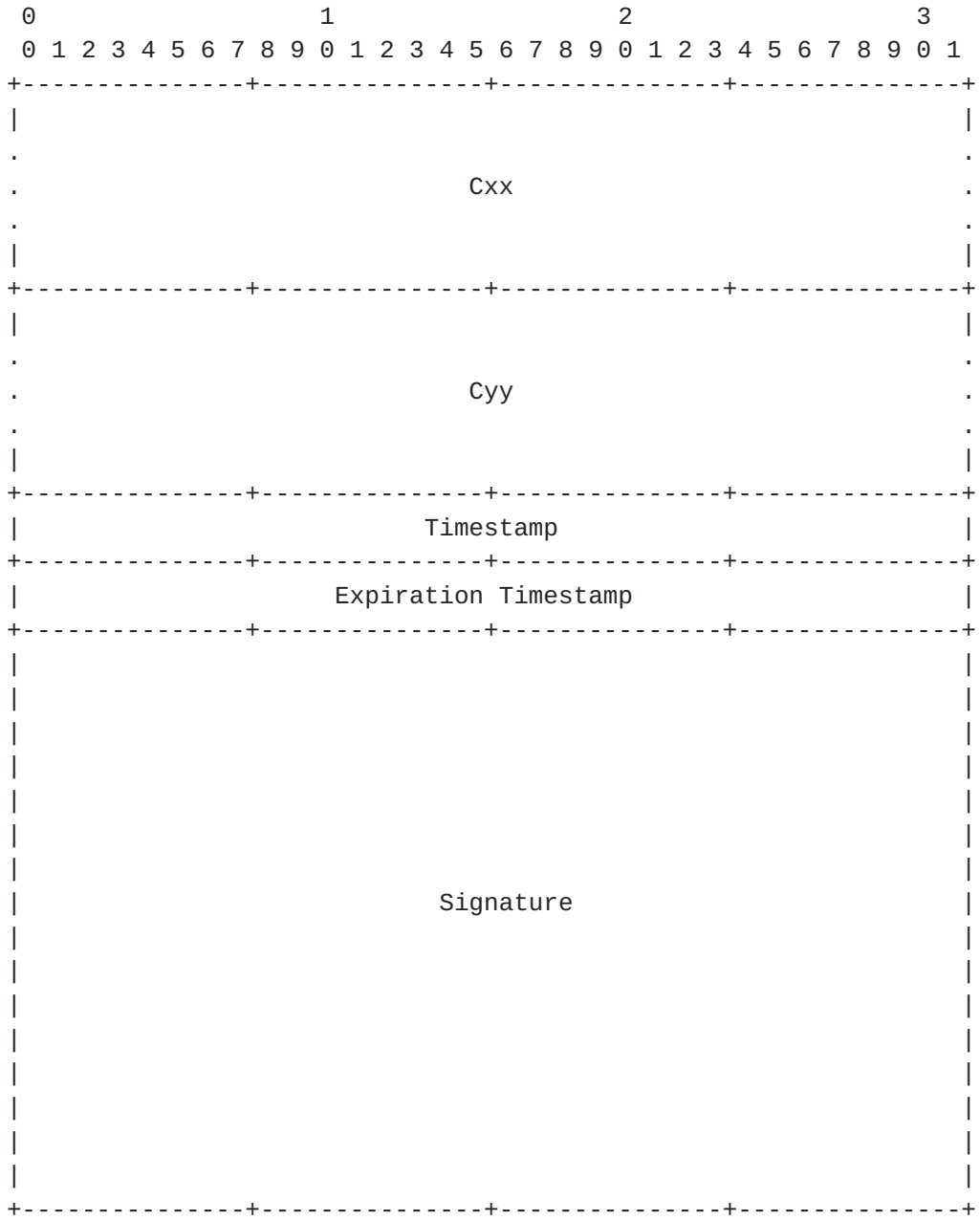


Figure 3: Certificate: X on Y

Cxy 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 certificates of this form have a length of 304 bytes. Certificate: Registry on Operator on Aircraft is unique in that is 680 bytes long, binding of two Cxy forms (in this specific case Certificate: Registry on Operator with Certificate: Operator on Aircraft).

3.2.1. Certificate: X on Y (Short Form)

This certificate is a special certificate that is the ultimate certificate of the DRIP UAS system. 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.

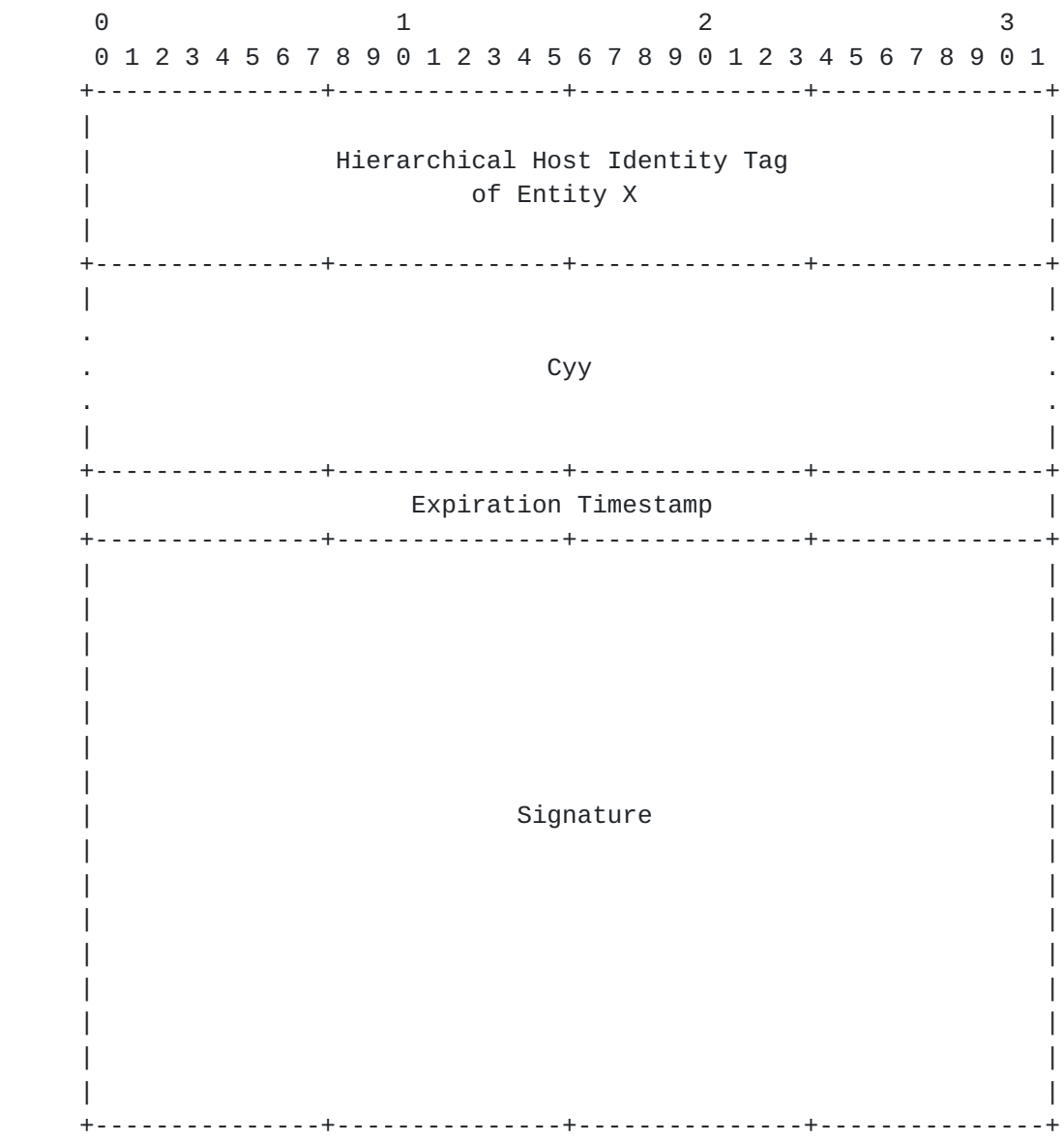


Figure 4: Certificate: X on Y (Short Form)

The short form of the Cxy this certificate 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.

Certificate: Registry on Aircraft is the main certificate in this class that is used in Broadcast RID using the HDAs HHIT and the Certificate: Aircraft on Aircraft for the current UAS ID.

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. 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 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 Security Considerations) 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. 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 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.

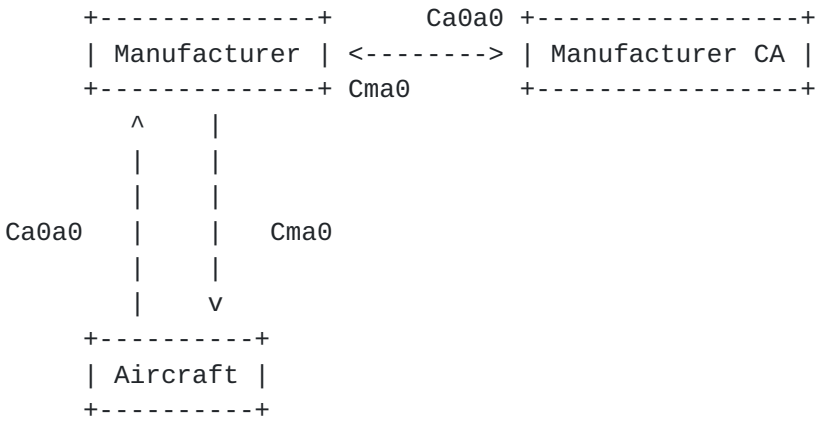
2 The entity sends to the Registry its HI for it to be hashed and result in the HHIT. The Registry would then either accept (returning the HHIT to the device) or deny this pairing.

In either case the Registry must decide 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 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 DRIP Certificates 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 and HHIT 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 (Certificate: Manufacturer on Aircraft 0) SHOULD be a DRIP Certificate in the Cxy Form - however this certificate could be a X.509 certificate binding the serial number to the manufacturer.

4.3. Registry

TODO

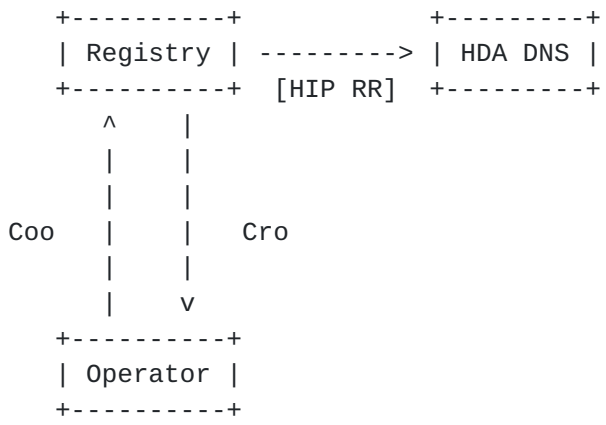
DRIP UAS RID defines two levels of hierarchy maintained by the Registration Assigning Authority (RAA) and HHIT Domain Authority (HDA). The authors anticipate that an RAA is owned and operated by a regional CAA (or a delegated party by an CAA in a specific airspace region) with HDAs being contracted out. 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. A Certificate: 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

certificate is generated (Certificate: 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 Certificate: 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.

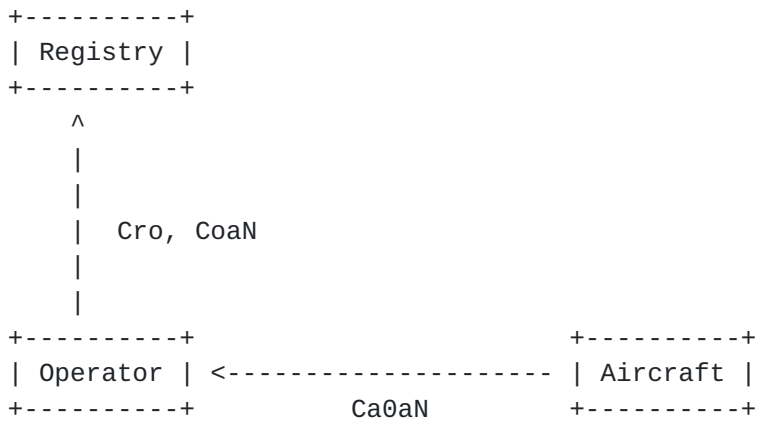


Figure 5: Standard Provision: Step 1

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 certificate (Certificate: Aircraft 0 on Aircraft N) is securely extracted by the Operator.

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

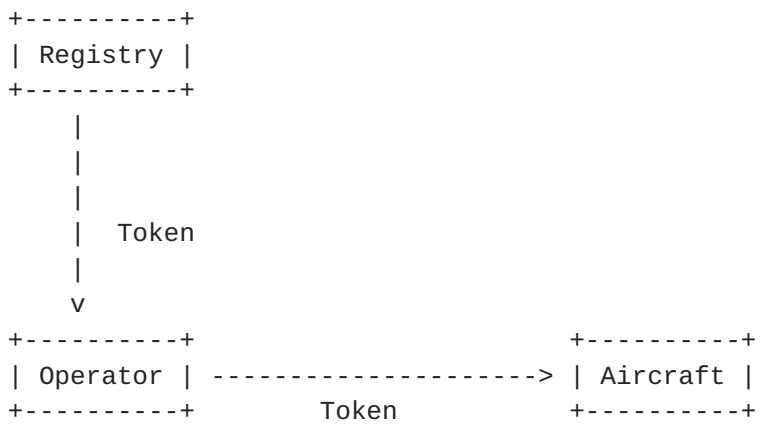


Figure 6: Standard Provision: Step 2

On the Registry Certificate: Registry on Operator is verified and used as confirmation that the Operator is already registered. Certificate: 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 Certificate: Manufacturer on Aircraft 0 and Certificate: Aircraft 0 to Aircraft N.

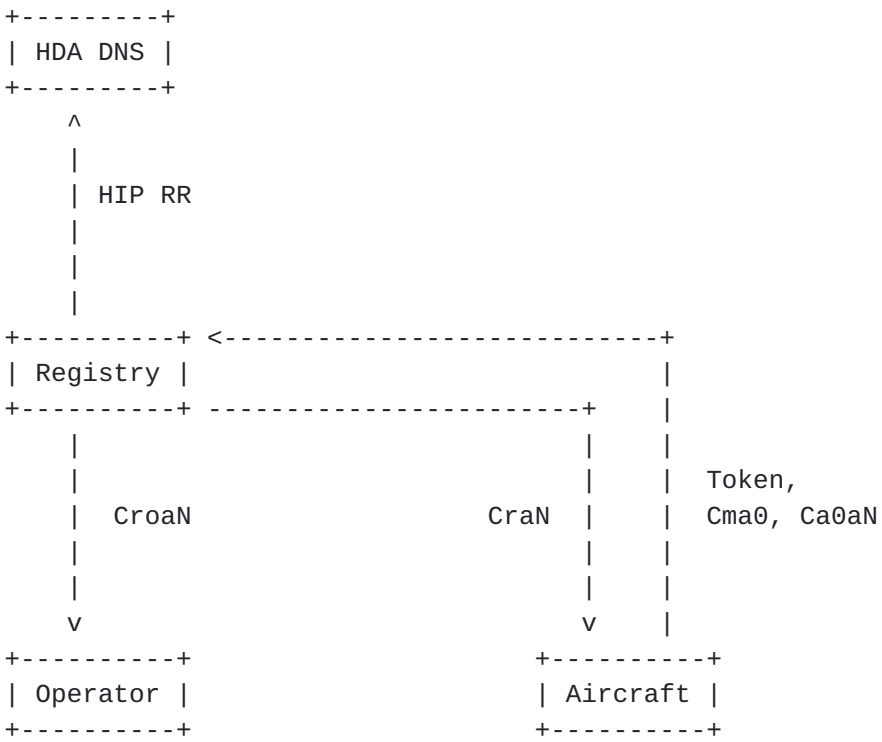


Figure 7: Standard Provision: Step 3

The Registry uses Certificate: Manufacturer on Aircraft 0 (with an external database if supported) to confirm the validity of the Aircraft. Certificate: Aircraft 0 on Aircraft N is correlated with Certificate: Operator on Aircraft N and Certificate: 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: Certificate: Registry on Operator on Aircraft N and Certificate: Registry on Aircraft N. A HIP RR (and other RR types as needed) are generated and inserted into the HDA.

Certificate: Registry on Operator on Aircraft N is sent via a secure channel back to the Operator to be stored. Certificate: Registry on Aircraft N 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.

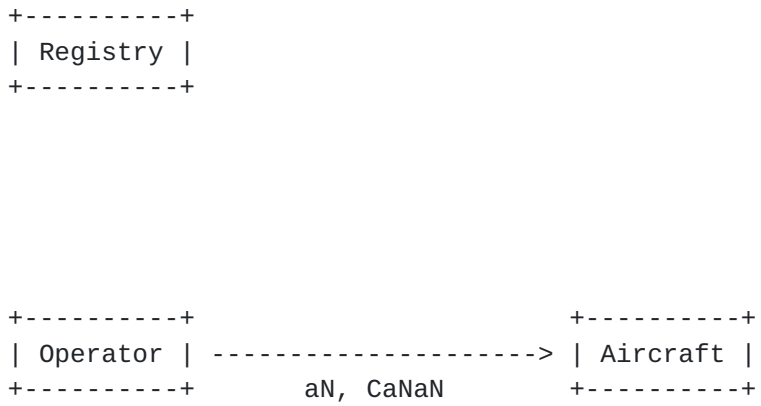


Figure 8: Operator Assisted Provision: Step 1

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 Certificate: Aircraft 0 on Aircraft N. After injecting the keypair and certificate, the Operator MUST destroy all copies of the keypair.

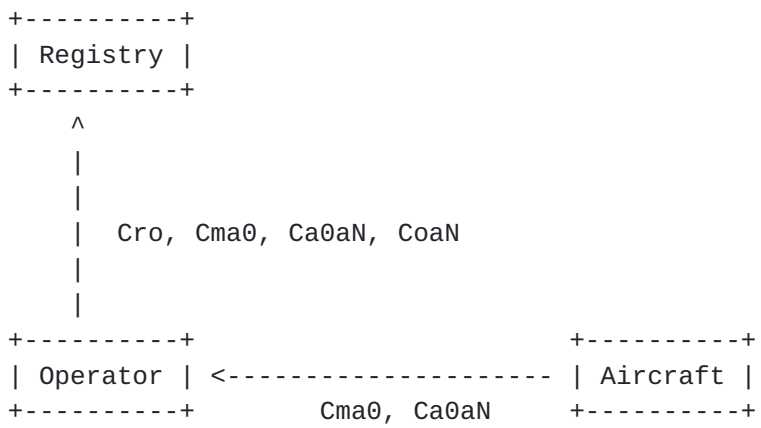


Figure 9: Operator Assisted Provision: Step 2

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

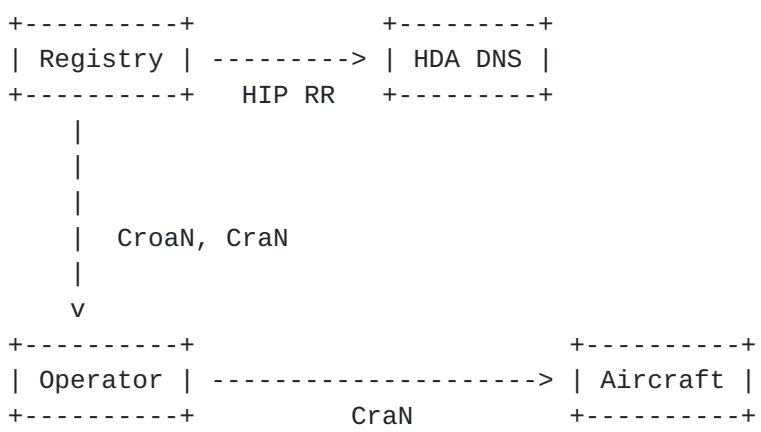


Figure 10: Operator Assisted Provision: Step 3

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

The Operator securely inject Certificate: Registry on Aircraft N and securely stores Certificate: 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 Certificate: Registry on Aircraft 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-05, 16 October 2020, <http://www.ietf.org/internet-drafts/draft-ietf-drip-reqs-05.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