

DRIP Registries

draft-wiethuechter-drip-registries-01

Adam Wiethuechter (AX Enterprize, LLC), Etal.

Updates since -00

- Expired Aug 2021
- Massively expanded (11 pages to 36 pages)
- Attestation definitions added
- Registry Classes/Entities
- Registry Operations
- Update Provisioning to use new Attestation forms

Overall, please excuse the mess – throwing all recent and old thoughts into one place to organize and share

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

Table of Contents	
1. Introduction	3
2. Terminology	4
2.1. Required Terminology	4
2.2. Definitions	4
3. Claims, Assertions, Attestations & Certificates	4
4. DRIP Attestations & Certificates	5
4.1. Attestation Structure	5
4.1.1. Attestor Identity Information	6
4.1.2. Attestation Data	6
4.1.3. Expiration Timestamp	7
4.1.4. Signing Timestamp	7
4.1.5. Signature	7
4.2. Attestations	7
4.2.1. Self-Attestation (SA-xx)	7
4.2.2. Attestation (A-xy)	8
4.2.3. Concise Attestation (CA-xy)	9
4.2.4. Mutual Attestation (MA-xy)	9
4.2.5. Link Attestation (LA-xy)	11
4.2.6. Broadcast Attestation (BA-xy)	12
4.3. Certificates	14
4.3.1. Attestation Certificate (AC-zxy)	14
4.3.2. Concise Certificate (CC-zxy)	15
4.3.3. Link Certificate (LC-zxy)	15
4.3.4. Mutual Certificate (MC-zxy)	16
5. Registries	17
5.1. Classes	17
5.1.1. Root	18
5.1.2. Registered Assigning Authorities	18
5.1.3. Hierarchical HIT Domain Authorities	18
5.2. Federation	19
6. DRIP Fully Qualified Domain Names	19
6.1. Serial Number	19
6.2. DET	19
7. Supported DNS Records	20
7.1. HIP RR	20
7.2. CERT RR	20
7.3. NS RR	20
7.4. AAAA RR	20
8. Registry Operations	20
8.1. Registering an RAA	21
8.1.1. Inputs	21
8.1.2. DNS Entries	21
8.1.3. Database Entries	21
8.1.4. Outputs	21
8.2. Registering an IRM	21
8.2.1. Inputs	22
8.2.2. DNS Entries	22
8.2.3. Database Entries	22
8.2.4. Outputs	22
8.3. Registering an HDA	22
8.3.1. Inputs	22
8.3.2. DNS Entries	23
8.3.3. Database Entries	23
8.3.4. Outputs	23
8.4. Registering an MRA	23
8.4.1. Inputs	23
8.4.2. DNS Entries	23
8.4.3. Database Entries	24
8.4.4. Outputs	24
8.5. Registering a Serial Number	24
8.5.1. Inputs	24
8.5.2. DNS Entries	24
8.5.3. Database Entries	24
8.5.4. Outputs	25
8.6. Registering an Operator	25
8.6.1. Inputs	25
8.6.2. DNS Entries	25
8.6.3. Database Entries	25
8.6.4. Outputs	25
8.7. Registering a Session ID	25
8.7.1. Inputs	26
8.7.2. DNS Entries	26
8.7.3. Database Entries	26
8.7.4. Outputs	26
9. Provisioning	27
9.1. Overview of Transactions	27
9.2. HHIT Delegation	28
9.3. Registry	29
9.4. Manufacturer	29
9.5. Operator	30
9.6. Aircraft	31
9.6.1. Standard Provisioning	31
9.6.2. Operator Assisted Provisioning	33
9.6.3. Initial Provisioning	35
10. Security Considerations	35
11. References	35
11.1. Normative References	35
11.2. Informative References	35
Authors' Addresses	36

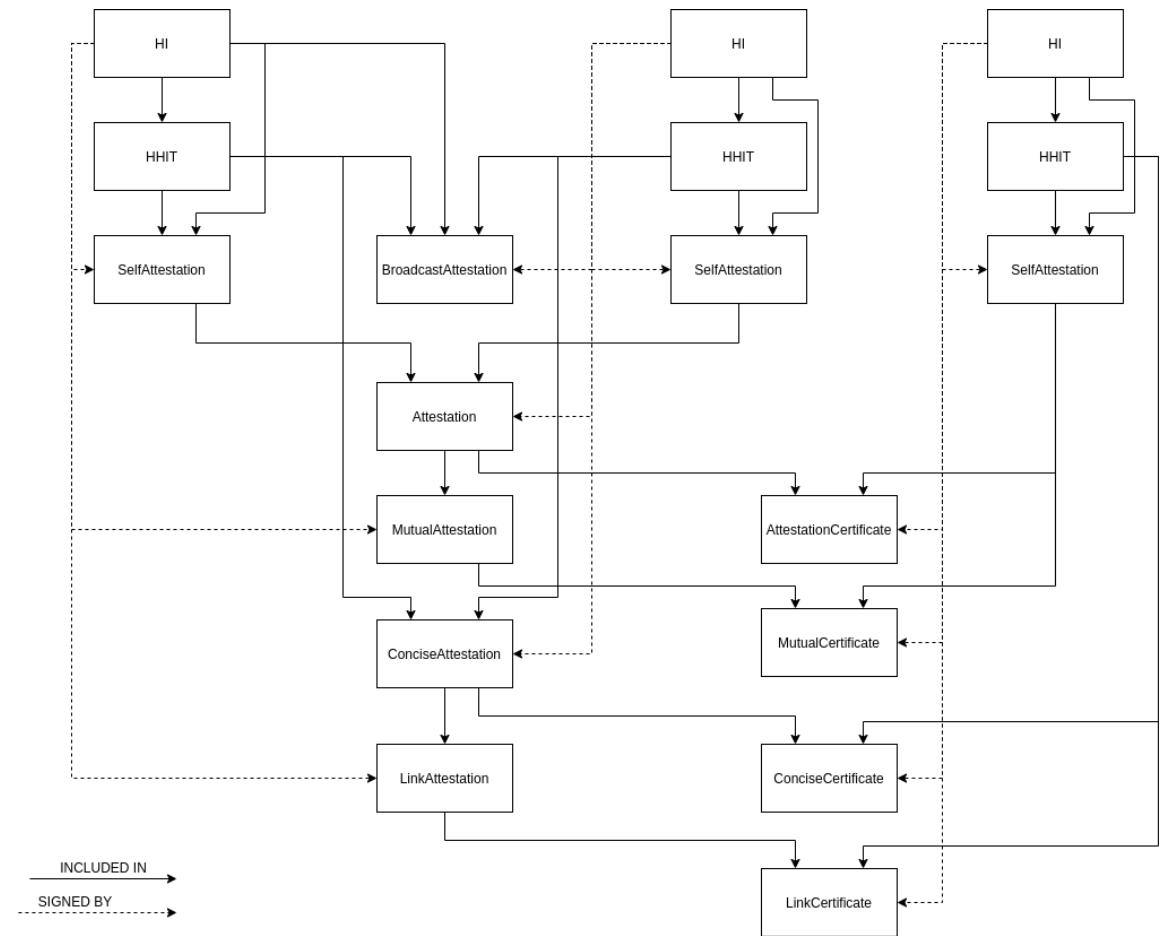
Text "Borrowed" from other DRIP drafts

- Definitions of Claims, Assertions, Attestations, Certificates
 - Trying to harmonize as in 3 different places (-arch, -uas-rid, -registries)
 - In line with -arch (do we remove from there and -uas-rid?)
- Section 4 was originally Appendix B of -auth
 - Expanded as needed with text and reorganized into subsections
 - Section 4.1 is new to this document

Attestations & Certificates



Figure 1: Attestation Structure

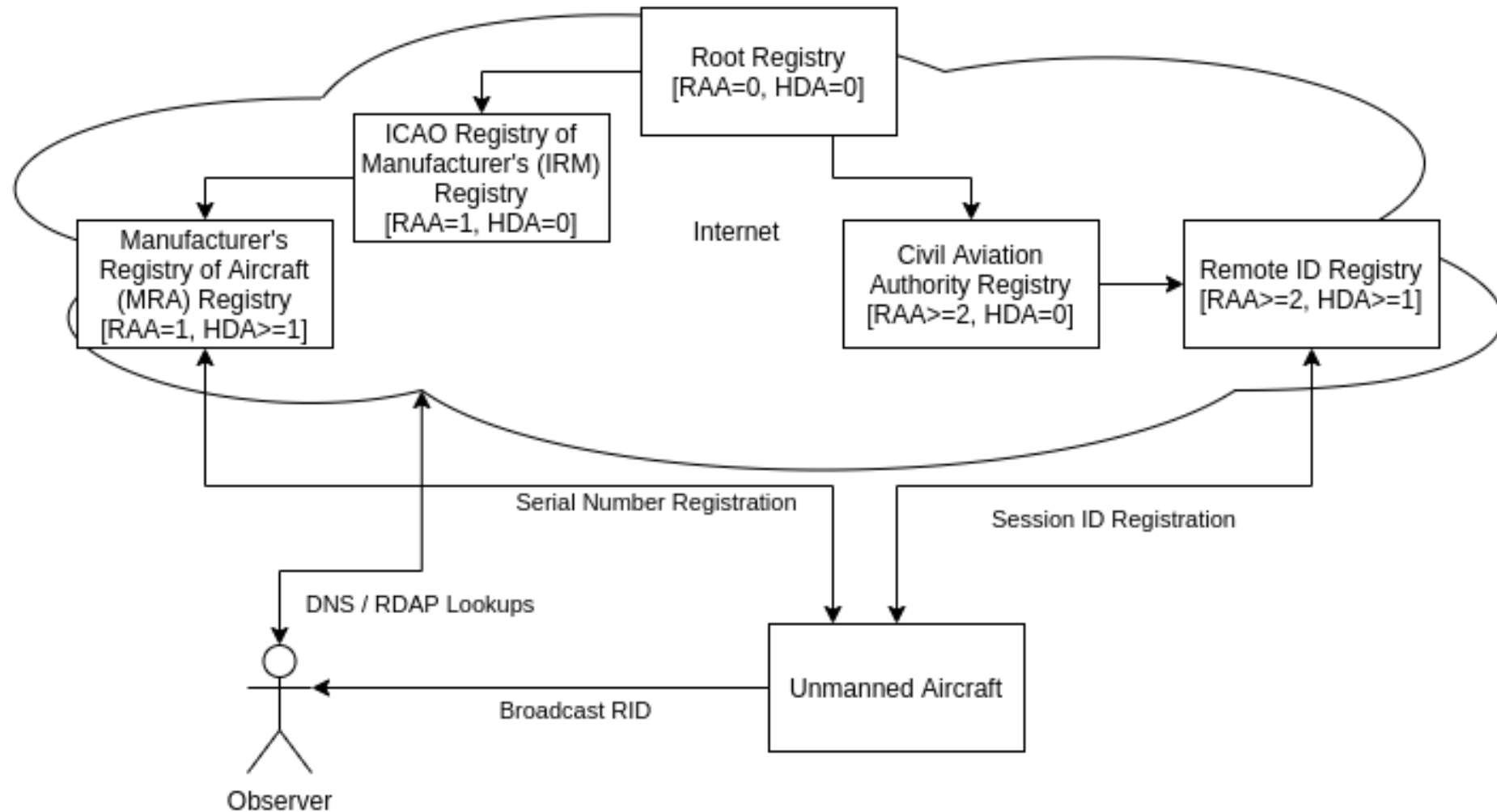


Registry Classes/Entities

Attempting to make a set of terms to make talking about registries easier

- Root - RAA=0, HDA=0
- RAAs
 - ICAO Registry of Manufacturer's (IRM) - RAA=1, HDA=0
 - Other RAAs (typically CAAs) - RAA=2+, HDA=0
- HDAs
 - Manufacturer's Registry of Aircraft (MRA) - RAA=1, HDA=1+
 - Remote ID Registries (RIDR) - RAA=2+, HDA=1+
 - perhaps useless/confusing classification?

Registry Tree Diagram



FQDN Definitions

For Serial Numbers and DETs

- Based on current prototype implementation at AX
 - Needs to harmonize with –uas-rid

Open questions:

- RAA/HDA format (int or hex)?
- Exploded (with padding) or Condensed IPv6 form?

6.1. Serial Number

```
Serial Number: 8653FZ2T7B8RA85D19LX
ICAO Mfr Code: 8653
Length Code: F
ID: FZ2T7B8RA85D19LX
FQDN: Z2T7B8RA85D19LX.F.8653.mfr.remoteid.aero
```

6.2. DET

```
DET: 2001:0030:00a0:0145:a3ad:1952:0ad0:a69e
ID: a3ad:1952:0ad0:a69e
OGA: 5
HDA: 0014 = 20
RAA: 000a = 10
FQDN: a3ad19520ad0a69e.5.20.10.det.remoteid.aero
```

DNS Records

- List of supported DNS RRs for DRIP
- Justification for their use
- NS RRs
 - Many different special forms and where they live
 - Determined from implementation prototyping to get lookups working properly

Registry Operations

- Biggest "new" section
- Hot mess of thoughts and notes
 - Needs massive rework to make "human" readable

Mostly a rehash of Section 9, but in a more technical sense defining end points and their mandatory/optional parameters

Implementation

Finally?!

AX Initial Prototype

- Deployed on a development Kub. Cluster
- Rough HTTP API to register
 - Registries, Operators, Aircraft (Serial Number and Session ID)
- "Manually" updates DNS zones
 - Started with BIND9, ended up with CoreDNS

Took over 4 months, due to other priorities but was used in last AX demo to register aircraft! DNS lookups worked, but not live (due to network constraints).

EPP / RDAP Progress

- EPP
 - Working on integrating with old prototype
 - Plan to pull XML tag definitions into draft for IANA considerations
 - Will need help on this as very confusing
 - Overall same results as original prototype but better
- RDAP
 - Starting soon...

TODOs / Next Steps

- Refine Section 4
- Section 8 needs help...
- Clean up and refine provisioning process
 - Are we missing anything?
 - Is very US centric – need EU inputs
- EPP/RDAP sections
 - EPP XML Tags and IANA Considerations associated with them
- PII protection (aka encryption of Serial Number and other things)

Plan to work with Bob M. extensively to add in the X.509 work and sort out other items.
This is the next major work item – important as supports –auth and –operator-privacy!
Adopt when?

Discussion

Questions, Comments, Concerns?



PEOPLE OFTEN USE ANCIENT TOOLS AND UIS TO DEVELOP MODERN CUTTING-EDGE TECHNOLOGY, BUT I DO IT THE OTHER WAY AROUND.

"I tried to train an AI to repair my Python environment but it kept giving up and deleting itself."

<https://xkcd.com/2510>