DRIP Identity Claims

draft-wiethuechter-drip-identity-claims-02

Adam Wiethuechter

DRIP WG – OCT20 Interim; 28 OCT 2020

From the DRIP Charter

DRIP’s goal is to specify how RID can be made trustworthy and available in both Internet and local-only connected scenarios

Overview

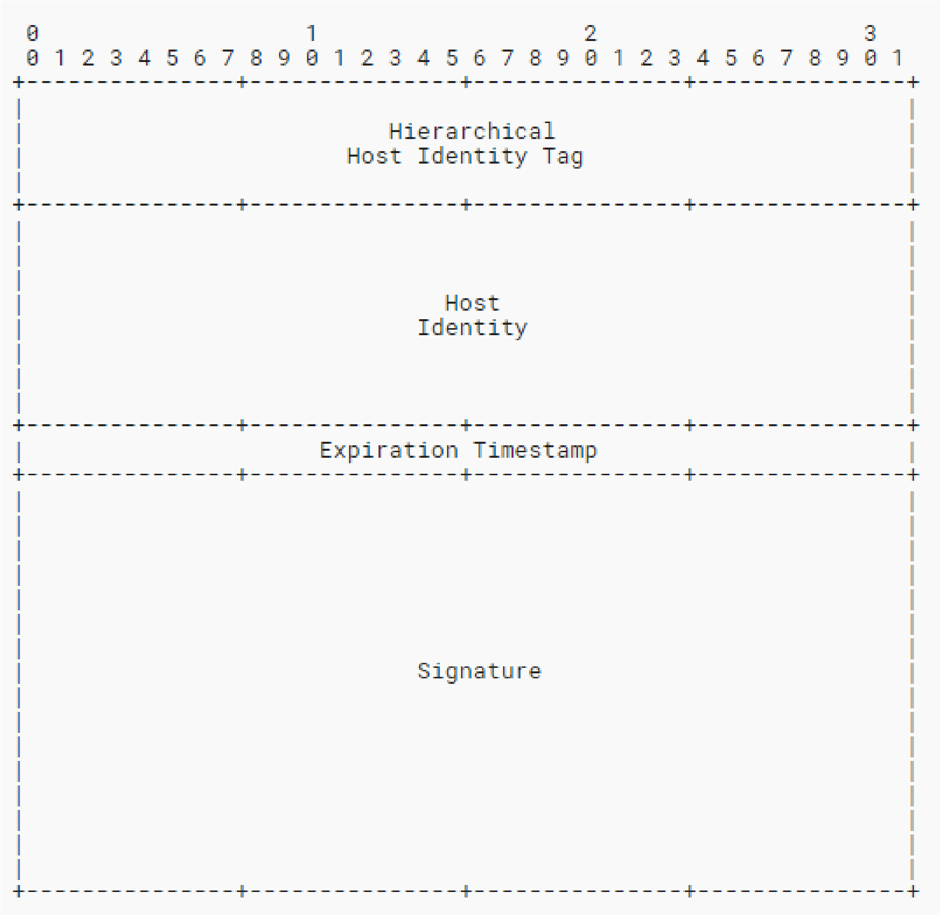
- Claim vs Certificate
  - Claim was chosen initially as “certificate” has a pre-establish connotation
  - Legal and technology baggage with the term and want to avoid confusion
  - This decision is in flux and we would like feedback on it! (we are now back on Certificate but Claims are reentering picture)
- Special to the UAS ecosystem for Remote ID
  - Asserts bindings between entities and objects
  - Created during provisioning of UA/Operator/Registry
- Draft name change?
  - Thinking DRIP Identity Proofs (to encompass both Certs and Claims)

Changes since v01

- Draft now written in Markdown
- Lots of text updated
  - Please re-review to find any missing things (such as references that were lost during MD conversion, etc.)
- Added Sections
  - Smaller form of Cxx found in Bob's UAS RID doc
  - Registry provisioning
- Generalized Cra into a Cxy (Short)

Form Cxx

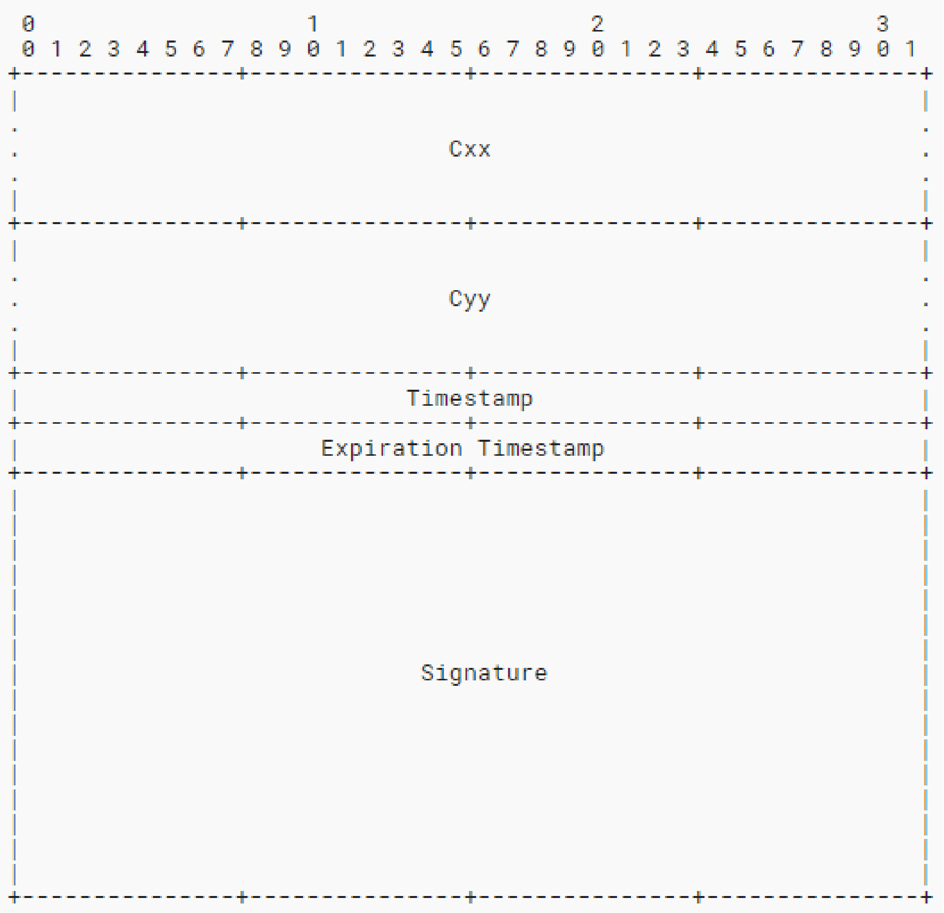
- Self-signed unverified claim
- Used to assert binding of HHIT/HI to a given entity (x)
  - Contains: HHIT, HI, Expiration Timestamp, Signature
  - 116 bytes in length
- Three specific entities:
  - Aircraft on Aircraft (Caa)
  - Operator on Operator (Coo)
  - Registry on Registry (Crr)
- Used in other forms



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|                                                               |
|                         Hierarchical                          |
|                      Host Identity Tag                        |
|                                                               |
+---------------+---------------+---------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                             Host                              |
|                           Identity                            |
|                                                               |
|                                                               |
|                                                               |
+---------------+---------------+---------------+---------------+
|                     Expiration Timestamp                      |
+---------------+---------------+---------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                           Signature                           |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------+---------------+---------------+---------------+
```

Form Cxy

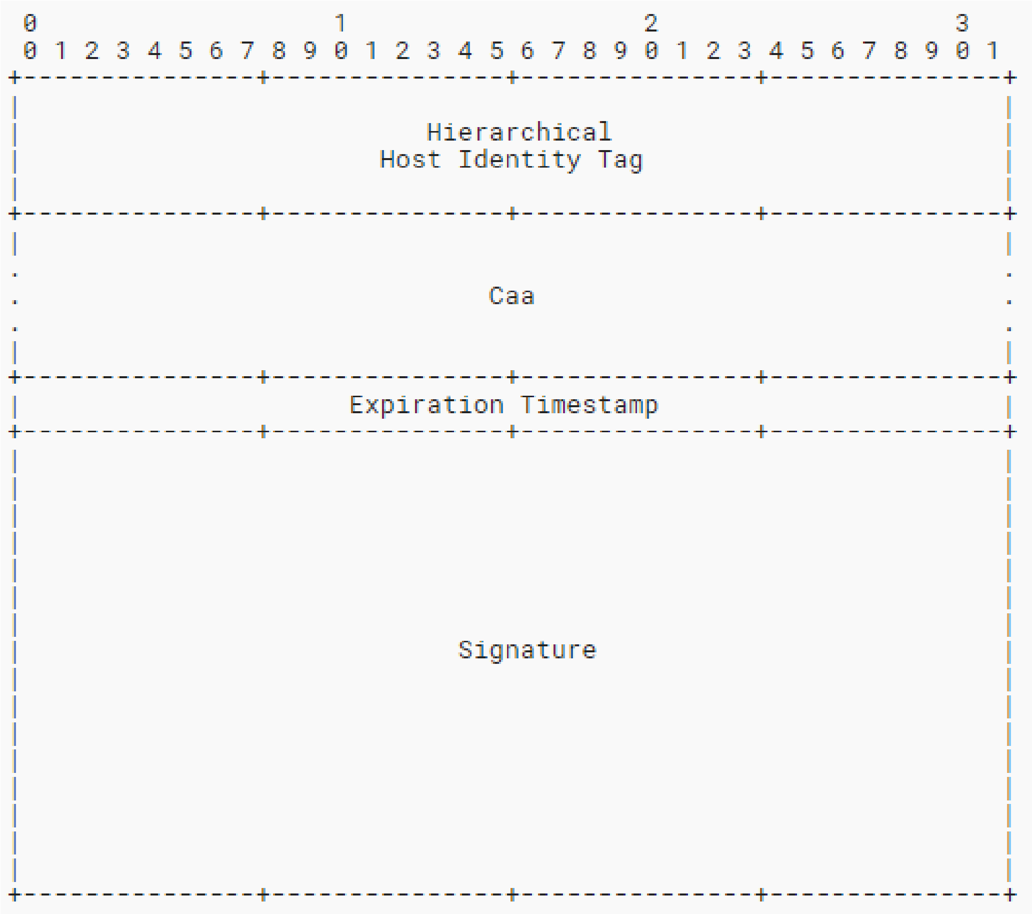
- Asserts binding between two entities (x and y)
  - Generally 'x' is an entity attesting 'y's claim (or adding a relationship)
  - Contains: Cxx, Cyy, Timestamp, Expiration Timestamp, Signature
  - 304/608 bytes in length
- 3 specific implementations of this form:
  - Registry on Operator (Cro)
  - Operator on Aircraft (Coa)
  - Registry on Operator on Aircraft (Croa)



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|                                                               |
.                                                               .
.                              Cxx                              .
.                                                               .
|                                                               |
+---------------+---------------+---------------+---------------+
|                                                               |
.                                                               .
.                              Cyy                              .
.                                                               .
|                                                               |
+---------------+---------------+---------------+---------------+
|                           Timestamp                           |
+---------------+---------------+---------------+---------------+
|                      Expiration Timestamp                     |
+---------------+---------------+---------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                           Signature                           |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------+---------------+---------------+---------------+
```

Certificate: Registry on Aircraft

- Special as it is used in authentication messages of Broadcast RID
  - Contains: HHIT of Registry, Caa, Expiration Timestamp, Signature
  - 200 bytes long
- Asserts the binding between a Registry and Aircraft

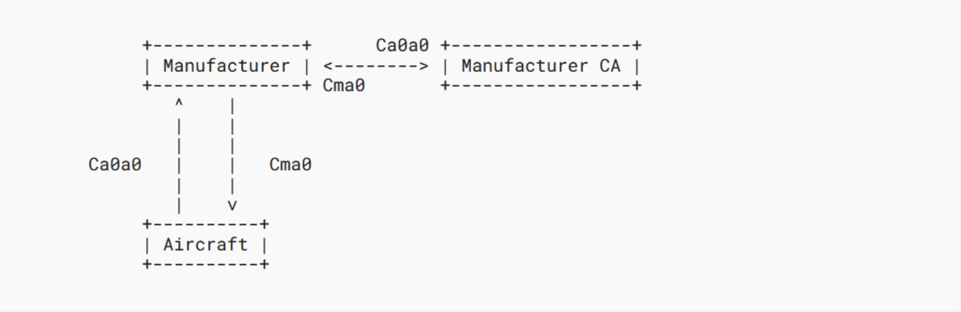


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|                                                               |
|                         Hierarchical                          |
|                       Host Identity Tag                       |
|                                                               |
+---------------+---------------+---------------+---------------+
|                                                               |
.                                                               .
.                             Caa                               .
.                                                               .
|                                                               |
+---------------+---------------+---------------+---------------+
|                     Expiration Timestamp                      |
+---------------+---------------+---------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                           Signature                           |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------+---------------+---------------+---------------+
```

Provisioning Process

Based on work in the DI WG for IATF under ICAO

Manufacturer Provisioning



```
         +--------------+       Ca0a0 +-----------------+
         | Manufacturer | <---------> | Manufacturer CA |
         +--------------+ Cma0        +-----------------+
             ^      |
             |      |
  Ca0a0      |      |      Cma0
             |      |
             |      v
         +----------+
         | Aircraft |
         +----------+
```

Aircraft CREATED

Manufacturer GENERATES: A0(A0_pub, A0_priv), C[A0, A0]

Manufacturer TX to Manufacturer CA: C[A0, A0]

Manufacturer CA GENERATES: C[M, A0]

This does not need to be a DRIP style certificate – it could be X.509!

Key point: ID (whatever it is) is being bound to Manufacturer!

Manufacturer CA TX to Manufacturer: C[M, A0]

Manufacturer INJECTS into Aircraft:A0(A0_pub, A0_priv), C[A0, A0], C[M, A0]

Aircraft PACKAGED

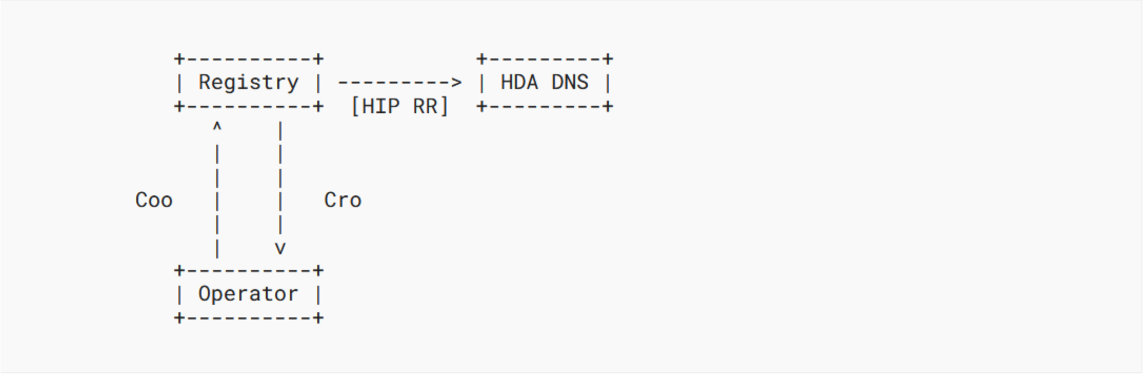
Aircraft SHIPPED to Retailer

Retailer SELLS Aircraft to Operator

Registry (RAA, HDA) Provisioning

- RAA GENERATES: R(R_pub, R_priv), C[R, R]
- HDA GENERATES: H(H_pub, H_priv), C[H, H]
- HDA TX to RAA: C[H, H]
- RAA CHECKS: C[H, H]
- RAA GENERATES using C[R, R] and C[H, H]: C[R, H]
- RAA TX to HDA: C[R, H]
  - Note from this point on Registry == HDA

Operator Provisioning



```
   +----------+             +---------+
   | Registry | ---------> | HDA DNS |
   +----------+  [HIP RR]  +---------+
       ^    |
       |    |
       |    |
 Coo   |    |    Cro
       |    |
       |    v
   +----------+
   | Operator |
   +----------+
```

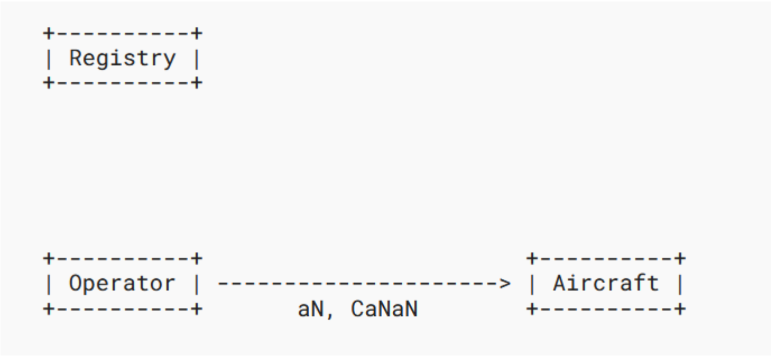
- Keypair generation
- HHIT derived from HI (public half of keypair)
  - Select Registry and use RAA/HDA to format valid HHIT
- Create Coo, send to Registry
- Registry perform verification check and adds HHIT/HI to DNS in the form of HIP RR
  - Verification check MUST include looking for HHIT collisions in current database of Registered HHITs
- Registry if successful, creates Cro and sends it back to Operator
- Registry if failed, sends error back asking to start over

Aircraft Provisioning (Operator Assisted)

Operator GENERATES: An(An_pub, An_priv), C[An, An]

Operator INJECTS into Aircraft: An(An_pub, An_priv), C[An, An]

Aircraft GENERATES using C[A0, A0] and C[An, An]: C[A0, An]



```
+----------+
| Registry |
+----------+




+----------+                       +----------+
| Operator | ----------------------> | Aircraft |
+----------+        aN, CaNaN        +----------+
```

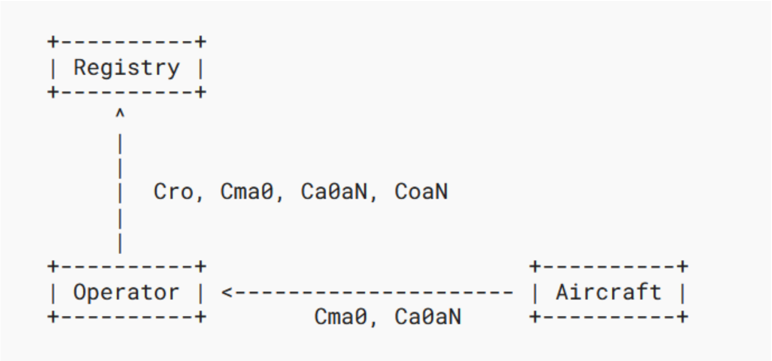
Operator EXTRACTS from Aircraft: C[M, A0], C[A0, An]

Operator GENERATES using C[O, O] and C[An, An]: C[O, An]

Operator TX to Registry: C[R, O], C[O, An], C[M, A0], C[A0, An]

Registry CHECKS: C[R, O], C[O, An], C[M, A0], C[A0, An]

C[M, A0] is checked using external systems (Manufacturer CA)



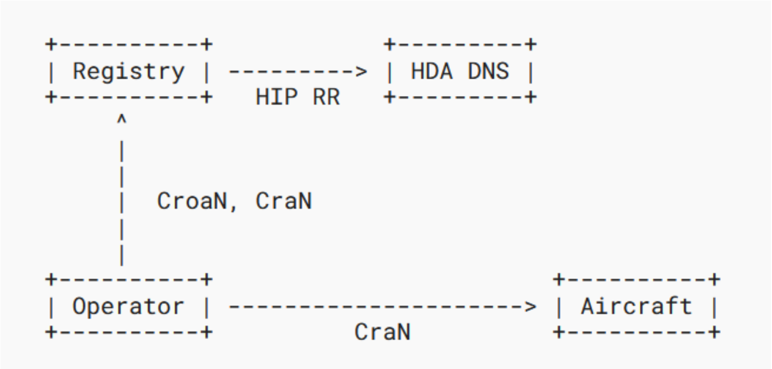
```
+----------+
| Registry |
+----------+
     ^
     |
     |
     |  Cro, Cma0, Ca0aN, CoaN
     |
     |
+----------+                       +----------+
| Operator | <---------------------- | Aircraft |
+----------+      Cma0, Ca0aN       +----------+
```

Registry GENERATES using C[H, H] and C[O, An] or C[A0, An]: C[R, O, An], C[R, An]

An is extracted from either C[O, An] or C[A0, An] and used to create C[R, An]

Registry TX to Operator: C[R, O, An], C[R, An]

Operator INJECTS into Aircraft: C[R, An]



```
+----------+           +---------+
| Registry | ---------> | HDA DNS |
+----------+   HIP RR   +---------+
     ^
     |
     |
     |  CroaN, CraN
     |
     |
+----------+                        +----------+
| Operator | ----------------------> | Aircraft |
+----------+          CraN          +----------+
```

Aircraft Provisioning

Operator COMMANDS Aircraft: GENERATE NEW KEYPAIR

Aircraft GENERATES: An(An_pub, An_priv), C[An, An]

Aircraft GENERATES using C[A0, A0] and C[An, An]: C[A0, An]

Operator EXTRACTS from Aircraft: C[An, An]

Operator GENERATES using C[O, O] and C[An, An]: C[O, An]

Operator TX to Registry: C[R, O], C[O, An]

Registry CHECKS: C[R, O]

Registry TX to Operator: P_TOKEN

Operator INJECTS into Aircraft: P_TOKEN

Operator COMMANDS Aircraft: CONTINUE PROVISIONING

Aircraft TX to Registry: P_TOKEN, C[M, A0], C[A0, An]

Registry CHECKS: P_TOKEN, C[M, A0], C[A0, An], C[O, An]

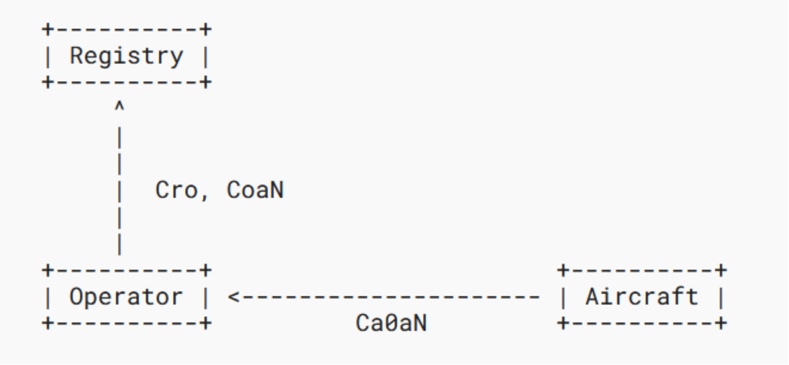
C[M, A0] is checked using external systems (Manufacturer CA)

Registry GENERATES using C[H, H] and C[O, An] or C[A0, An]: C[R, O, An], C[R, An]

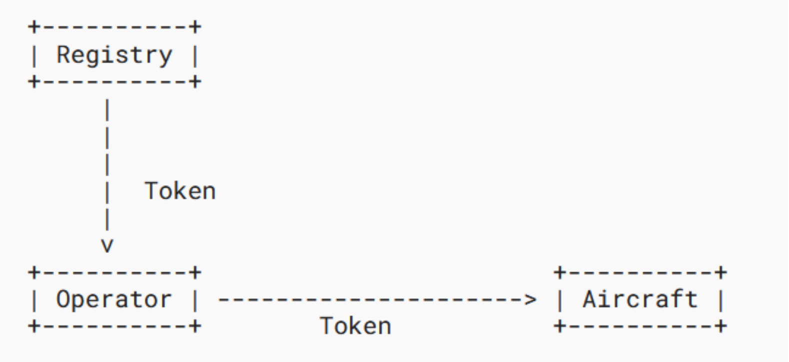
An is extracted from either C[O, An] or C[A0, An] and used to create C[R, An]

Registry TX to Operator: C[R, O, An]

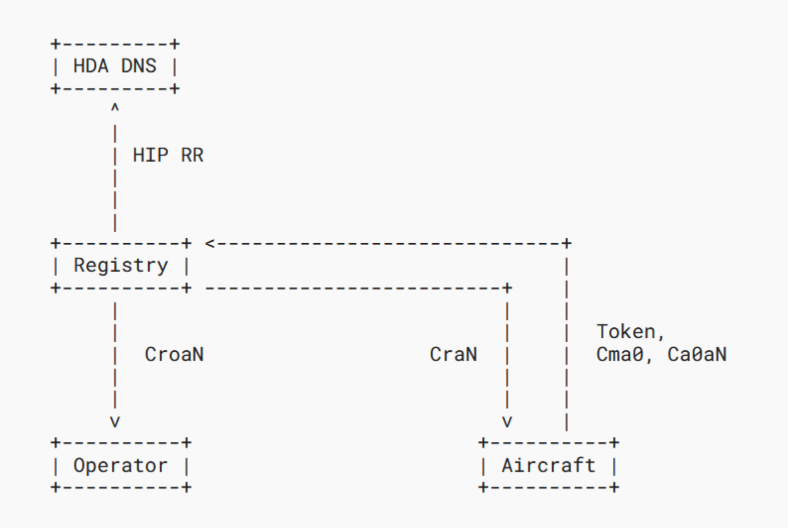
Registry TX to Operator: C[R, An]



```
+----------+
| Registry |
+----------+
     ^
     |
     |
     |   Cro, CoaN
     |
     |
+----------+                        +----------+
| Operator | <--------------------- | Aircraft |
+----------+         Ca0aN          +----------+
```



```
+----------+
| Registry |
+----------+
     |
     |
     |
     |   Token
     |
     v
+----------+                        +----------+
| Operator | ---------------------> | Aircraft |
+----------+         Token          +----------+
```

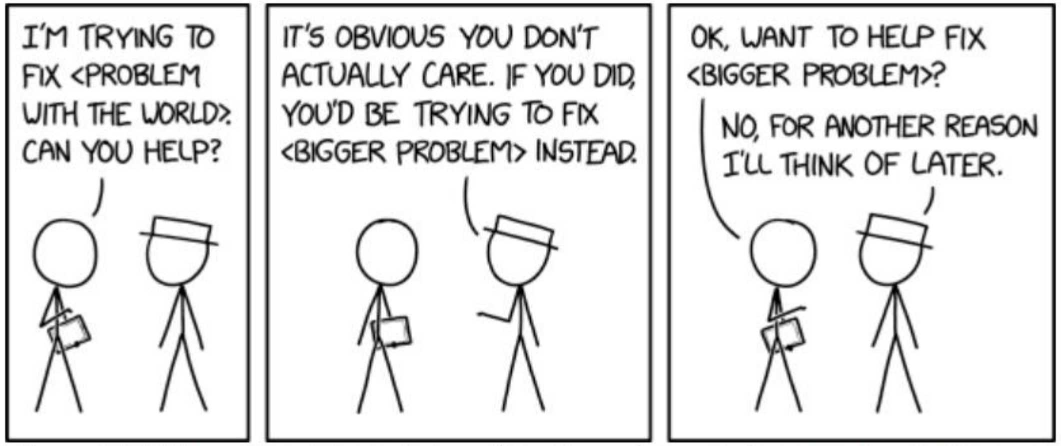


```
+---------+
| HDA DNS |
+---------+
     ^
     |
     | HIP RR
     |
     |
     |
+----------+ <--------------------------+
| Registry |                            |
+----------+ ----------------------+    |
     |                             |    |
     |                             |    |   Token,
     |   CroaN               CraN  |    |   Cma0, Ca0aN
     |                             |    |
     |                             |    |
     v                             v    |
+----------+                     +----------+
| Operator |                     | Aircraft |
+----------+                     +----------+
```

New Details (Draft TODOs)

- Bob has brought up Timestamp considerations
  - Use a Current Timestamp instead of Expiry Timestamp
  - Add separate forms switching or having both?
- Offline Self-Claim should be added?
  - (UA HHIT | UA HI | HDA HHIT | HDA Expiry TS | HDA Sig) | UA Expiry TS | UA Sig
    - Only first portion here (in parenthesis), rest in Auth Draft
- How to handle provisioning of those who create own software?
- Ordering of Cxy fields?

Bigger Problem


I'M TRYING TO FIX <PROBLEM WITH THE WORLD>. CAN YOU HELP?
IT'S OBVIOUS YOU DON'T ACTUALLY CARE. IF YOU DID, YOU'D BE TRYING TO FIX <BIGGER PROBLEM> INSTEAD.
OK, WANT TO HELP FIX <BIGGER PROBLEM>?
NO, FOR ANOTHER REASON I'LL THINK OF LATER.

Title text: Your point that the world contains multiple problems is a real slam-dunk argument against fixing any of them.

https://xkcd.com/2368/

Discussion

Questions, Comments, Concerns?