# DRIP Identity Claims

draft-wiethuechter-drip-identity-claims-00

Adam Wiethuechter

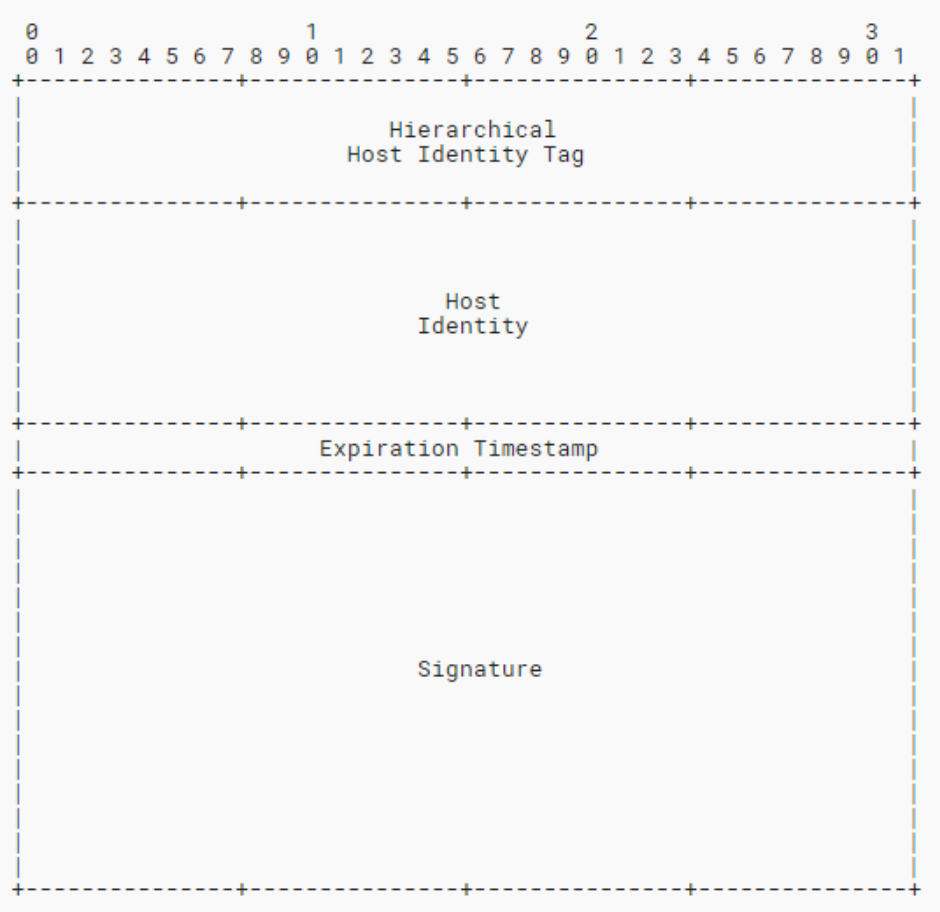
DRIP WG – IETF 107; March 25, 2020

# Overview

- Claim vs Certificate
  - Claim was chosen 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!
- Special to the UAS ecosystem for Remote ID
  - Asserts bindings between entities and objects
  - Created during provisioning of UA/Operator/Registry

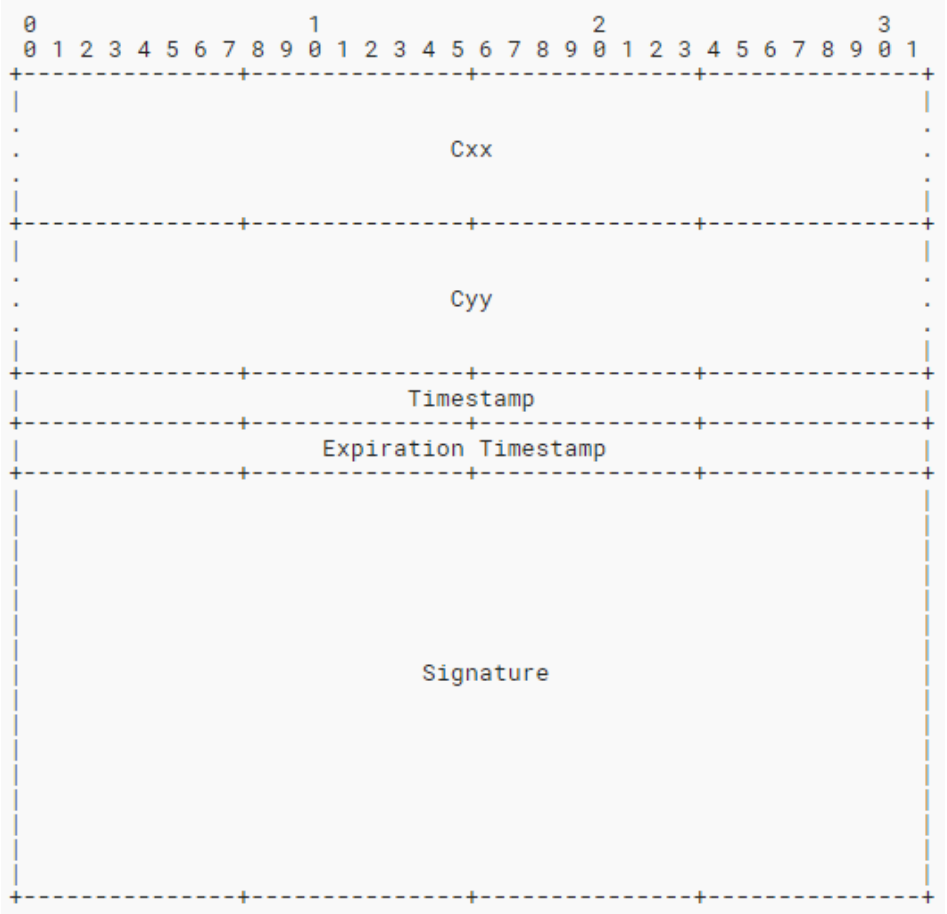
# Form Cxx

- 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 claims:
  - Aircraft on Aircraft (Caa)
  - Operator on Operator (Coo)
  - Registry on Registry (Crr)
- Used in other claim forms



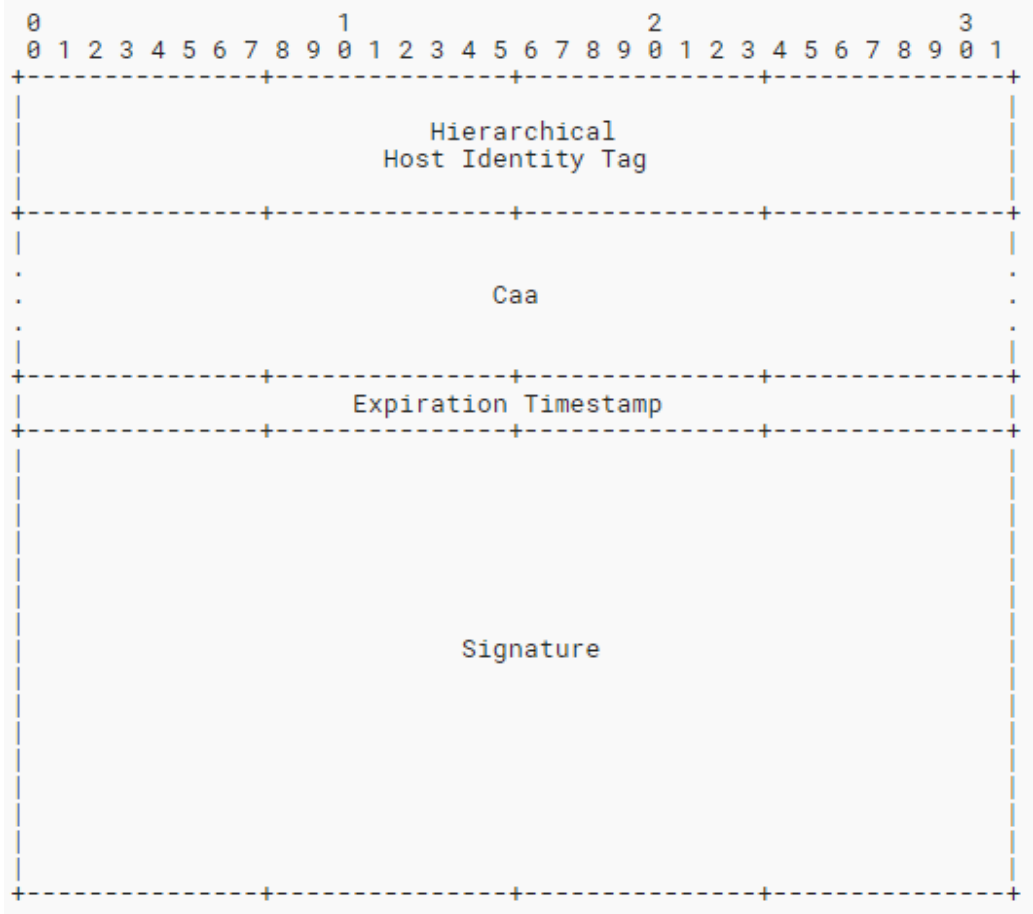
# Form Cxy

- 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 claims of this form:
  - Registry on Operator (Cro)
  - Operator on Aircraft (Coa)
  - Registry on Operator on Aircraft (Croa)

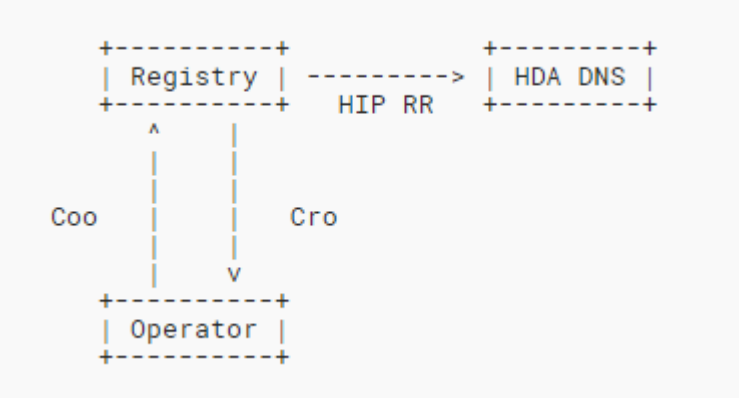


# Claim: Registry on Aircraft

- 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

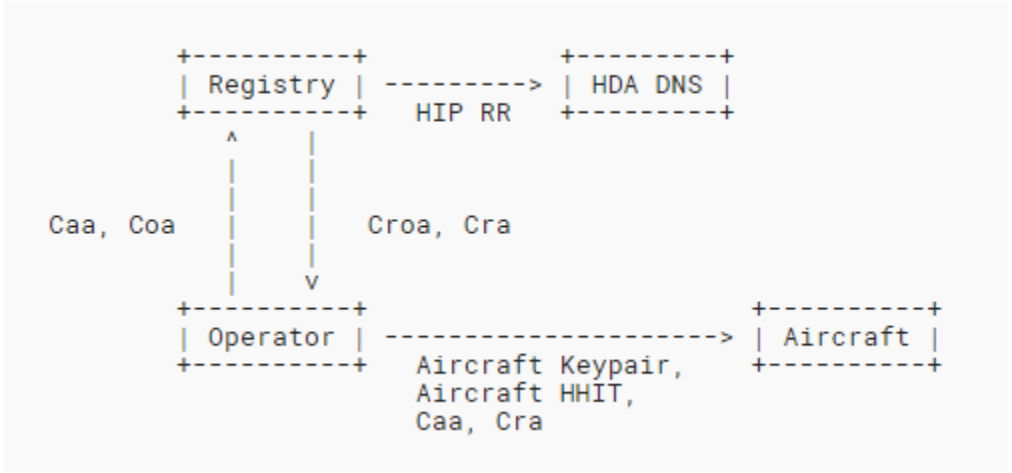


# Provisioning: Operator




- Keypair generation
- HHIT derived from HI (public half of keypair)
  - Select Registry and use RRA/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

# Provisioning: Aircraft




- Keypair generation
- HHIT derived from HI (public half of keypair)
  - Registry selected and RRA/HDA used to format valid HHIT
- Create Caa, create Coa
- Send Caa, Coa 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 Croa, Cra and sends them back
- Registry if failed, sends error back asking to start over


https://xkcd.com/364/

# Discussion

Questions, Comments, Concerns?