Trustworthy Multipurpose Remote Identification (tm-rid) Interim Webex 2010 FEB 06 THU: Proposed Architecture

Stu Card, Adam Wiethuechter

Progress & Next Steps to add strong authentication techniques to identify physically nearby objects

Terminologies of the 2 worlds collide

UAS (ASTM & CAAs)

- UA: Unmanned Aircraft
- GCS: Ground Control Station
- UAS: Unmanned Aircraft System (UA + GCS)
- USS: UTM Service Supplier
- SDSP: Supplemental Data Service Provider
- UTM: UAS Traffic Management
- UVR: UAS Volume Reservation
- UAS RID: UAS Remote Identification
- TMRID: Trustworthy Multipurpose Remote ID

Internet (IETF & ICANN)

- DNS: Domain Name System
- RR: Resource Record (in DNS)
- WHOIS: domain name registry lookup tool
- RDAP: Registry Data Access Protocol
- EPP: Extensible Provisioning Protocol
- HIP: Host Identity Protocol
- [H]HI[T]: [Hierarchical] Host Identity [Tag]
- Certificate: HHIT + HI, w/expiration, signed w/HI(priv)
  - Cxy is a certificate signed by Entity X, attesting to the veracity of a claim made by Entity Y

Unmanned Aircraft System (UAS) Remote Identification (RID): Motivation for Proposed Architecture

Recap…

- ASTM F38.02 WK65041 UAS RID… Broadcast RID… Network RID…
- FAA (US) NPRM… Standard RID… Limited RID… error correction… cybersecurity… also EASA (EU) regs soon to take effect…
- Leverage existing Internet services/infrastructure/protocols (e.g. WHOIS/RDAP, EPP, DNS, HIP).

  Strengthen authentication, balance operator privacy w/genuine Need To Know…
- (UA physical location : UA ID) ~ (host logical location (IP) : host ID)
  - ✓ We have prototyped & flown a HIP based extension to OpenDroneID.
  - ❑ Manufacturer assigned Hardware Serial Number per ANSI/CTA-1063-A (ASTM UAS ID Type 1)
  - ❑ UTM system assigned Session ID (ASTM UAS ID Type 3 UUID): “randomly-generated alphanumeric code that is used only for one flight” (p. 21, NPRM)

UPP2 Use Case 4

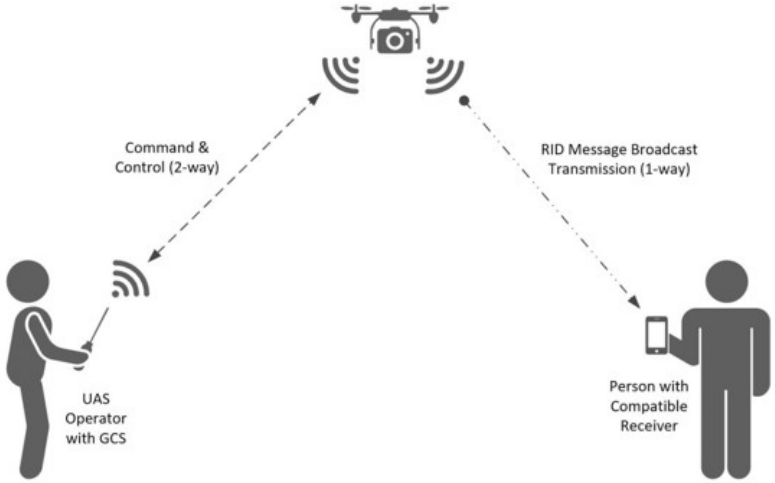


Figure 9-2: Remote ID Message Transmission via Broadcast

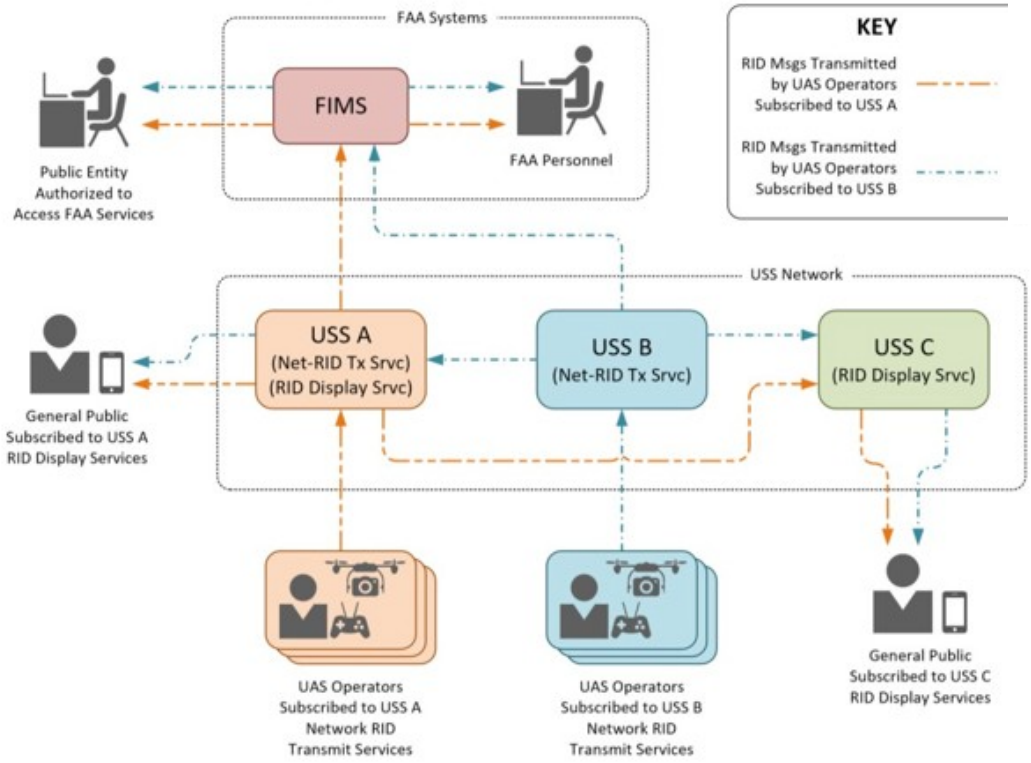


Figure 9-1: Remote ID Message Transmission via Network Publication Flow

AXE UPP2 Use Case 5

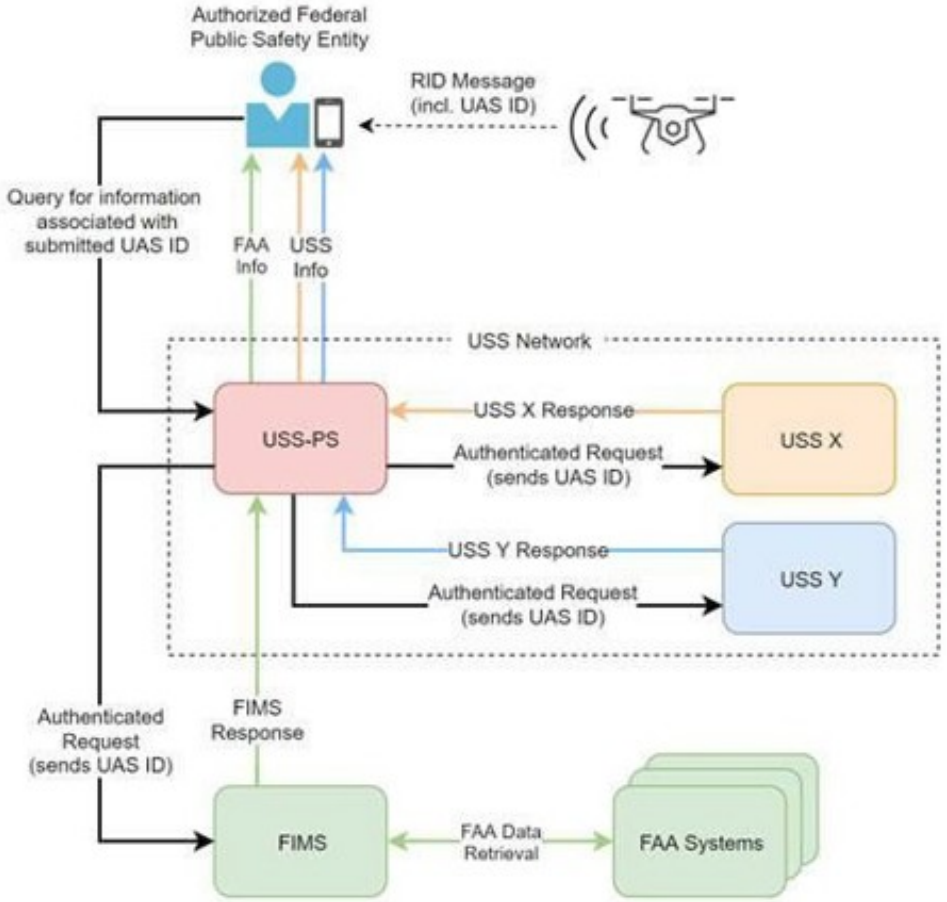


Figure 10-1: Direct Query to FAA and USS Network

Goal: Make RID Received Information *Immediately Actionable* -> Sub-Goals

- make it trustworthy (despite severe constraints of Broadcast RID)
- enable verification that an UAS is registered

  if so, in which registry (for classification of trusted operators on the basis of known registry vetting, even by observers lacking Internet connectivity at observation time)
- enable instant establishment, by authorized parties, of secure communications with the remote pilot

tm-rid General Req's for UAS

1. verify that messages originated from the claimed sender
2. verify that the UAS ID is in a registry & identify which one
3. lookup, from the UAS ID, public information
4. lookup, w/AAA, per policy, private information
5. structure information for both human and machine readability
6. provision registries with
    1. static information on the UAS & its Operator / Pilot In Command / Remote Pilot
    2. dynamic information on its current operation within the UTM
    3. Internet direct contact information for services related to the foregoing
7. close the AAA-policy registry loop by
    1. governing AAA per registered policies
    2. administering policies only via AAA
8. dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

tm-rid General Req's for UAS *easily satisfied* if UAS ID is a HHIT in DNS & Whois (w/RDAP, EPP & XACML)

1. verify that messages originated from the claimed sender
2. verify that the UAS ID is in a registry & identify which one
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

tm-rid General Req's for UAS *easily satisfied* if UAS ID is a HHIT **w/proposed new crypto** in DNS & Whois

1. ***verify that messages originated from the claimed sender***
2. ***verify that the UAS ID is in a registry & identify which one***
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

tm-rid General Req's for UAS *easily satisfied* if UAS ID is a HHIT w/proposed new crypto in DNS & Whois, **plus HIP is deployed on participating UTM nodes**

1. *verify that messages originated from the claimed sender*
2. *verify that the UAS ID is in a registry & identify which one*
3. *lookup, from the UAS ID, public information*
4. *lookup, w/AAA, per policy, private information*
5. *structure information for both human and machine readability*
6. *provision registries with*
    1. *static information on the UAS & its Operator / Pilot In Command / Remote Pilot*
    2. *dynamic information on its current operation within the UTM*
    3. *Internet direct contact information for services related to the foregoing*
7. *close the AAA-policy registry loop by*
    1. *governing AAA per registered policies*
    2. *administering policies only via AAA*
8. ***dynamically establish, w/AAA, per policy, E2E strongly encrypted communications w/the UAS RID sender & entities looked up from the UAS ID, inc. the GCS & USS***

It is highly desirable that Broadcast RID receivers also be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. distributed ledger), *inter alia* for correlation to assess sender & receiver veracity.

tm-rid Req's for UAS Identifiers

1. 20 bytes or smaller
2. sufficient to identify a registry in which the UAS is listed
3. sufficient to enable lookup of other data in that registry
4. unique within a to-be-defined scope
5. non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID).

- A tm-rid UAS ID MUST NOT facilitate adversarial correlation of UAS operational patterns; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support defined scalable timely registration methods.

- Mechanisms standardized in tm-rid MUST be capable of proving ownership of a claimed UAS ID, and SHOULD be capable of doing so immediately on an observer device lacking Internet connectivity at the time of observation.

- Mechanisms standardized in tm-rid MUST be capable of verifying that messages claiming to have been sent from a UAS with a given UAS ID indeed came from the claimed sender.

tm-rid Req's for UAS Identifiers *satisfied* by a HHIT in DNS & Whois (w/RDAP, EPP & XACML)

1. *20 bytes or smaller*
2. *sufficient to identify a registry in which the UAS is listed*
3. *sufficient to enable lookup of other data in that registry*
4. *unique within a to-be-defined scope*
5. *non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID)*

- A tm-rid UAS ID MUST NOT facilitate adversarial correlation of UAS operational patterns; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support defined scalable timely registration methods.

- *Mechanisms standardized in tm-rid MUST be capable of proving ownership of a claimed UAS ID, and SHOULD be capable of doing so immediately on an observer device lacking Internet connectivity at the time of observation.*

- *Mechanisms standardized in tm-rid MUST be capable of verifying that messages claiming to have been sent from a UAS with a given UAS ID indeed came from the claimed sender.*

tm-rid Req's for UAS Identifiers *satisfied* by a HHIT in DNS & Whois (w/RDAP, EPP & XACML) **used for only 1 UAS flight**

1. *20 bytes or smaller*
2. *sufficient to identify a registry in which the UAS is listed*
3. *sufficient to enable lookup of other data in that registry*
4. *unique within a to-be-defined scope*
5. *non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID)*

- ***A tm-rid UAS ID MUST NOT facilitate adversarial correlation of UAS operational patterns; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support defined scalable timely registration methods.***

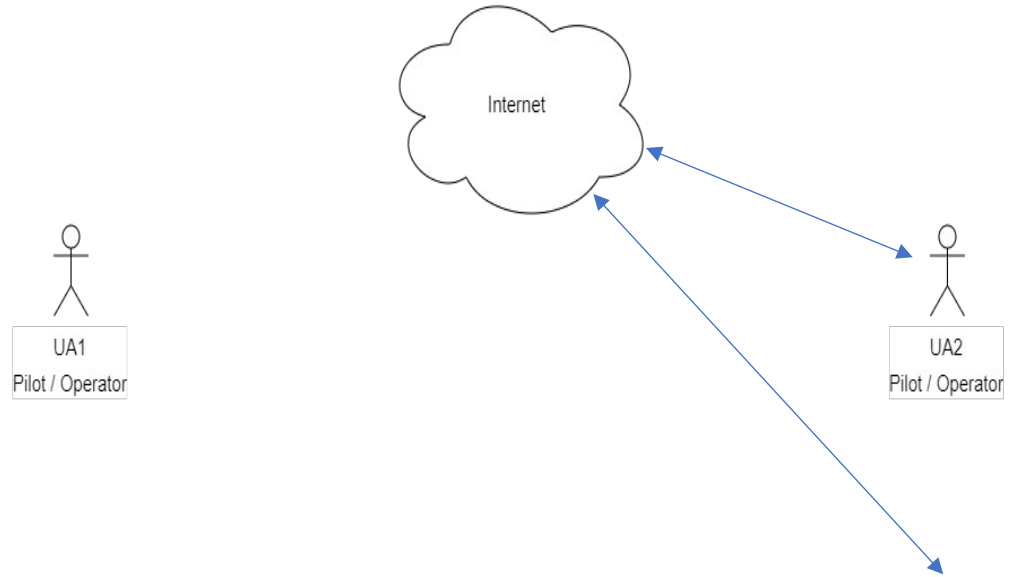
- *Mechanisms standardized in tm-rid MUST be capable of proving ownership of a claimed UAS ID, and SHOULD be capable of doing so immediately on an observer device lacking Internet connectivity at the time of observation.*

- *Mechanisms standardized in tm-rid MUST be capable of verifying that messages claiming to have been sent from a UAS with a given UAS ID indeed came from the claimed sender.*

Encode a HHIT as an ASTM UAS ID Type 1

- Comply w/ANSI-CTA-2063-A.
- Set length field to “F” encoding value 15.
- In 15 character serial “number” field, encode:
  - last nibble of IANA HHIT prefix (1 char);
  - ORCHID Generating Algorithm ID (1 char);
  - 64 bit hash of HI (13 chars, 5 bits each).
- In DNS, map 4 character Manufacturer ID to a HHIT registry (RRA + HDA).
- Also map UAS ID Type 3 values to HHITs in DNS: big questions of scalability?

tmrid: operator registration



Operator generates HI keypair (**HIo** / **HIo(priv)**) along with cert **Coo**. Operator sends **Coo** to Registry.

Registry validates **Coo** and makes decision to add Operator to Registry.
Registry (using its HI keypair) will create **Cro** and securely sends it back to Operator for confirmation.

tmrid: ua registration

General Public Observer

Public Safety Observer

(5) Operator securely embeds UA keypair and **Cra** into UA

Internet

(2) Operator sends, **Caa** and **Coa** to Registry

UA1
Pilot / Operator

UA2
Pilot / Operator

(1) Operator creates HI keypair for UA (**HIa** / **HIa(priv)**), generates cert **Caa** using them.
Operator using *his keypair* creates **Coa.**

(3.5) Registry adds HHIT and other info to DNS

(4) Croa and **Cra** are transmitted securely back to Operator/UA

(3) Registry validates **Caa**, plus inspects **Coa** and makes decision to add UA to Registry.
Registry (using its HI keypair) creates **Croa** as proof of registration of UA to Operator.
Registry also creates **Cra** to be

Public Registry

DNS

Private Registry

tmrid: message authentication w/o Internet

UA Broadcasts **Cra** and other messages (e.g. position + velocity) signed w/**HIa(priv)**

General Public Observer

Public Safety Observer

Not Needed!

X

X

Internet

Observers verify signatures, ensuring received data (e.g. position track) all really came from UA w/claimed ID

UA1 Pilot / Operator

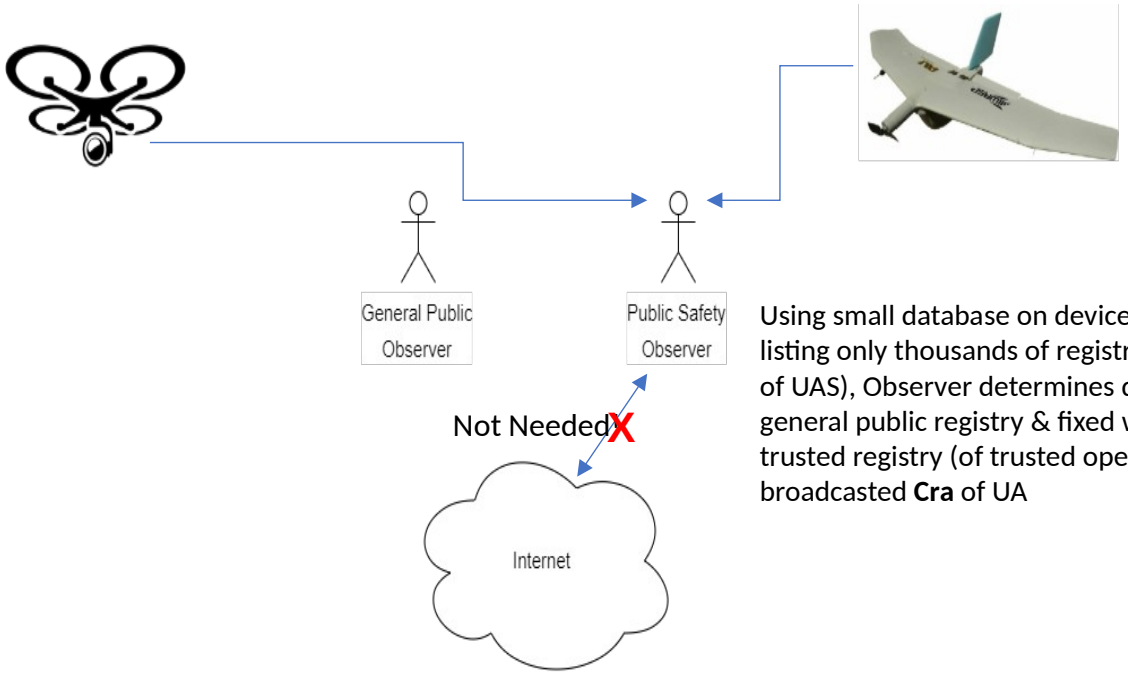
UA2 Pilot / Operator

Public Registry

DNS

Private Registry

tmrid: operator trust classification w/o Internet



Using small database on device (e.g., phone) listing only thousands of registries (not millions of UAS), Observer determines quadcopter is in general public registry & fixed wing in Observer trusted registry (of trusted operators) using broadcasted **Cra** of UA

tmrid: Observer to Operator or Pilot or Proxy (O2P2) comms

(1)

General Public Observer

Public Safety Observer

Observer w/credentials satisfying access control policy instantly establishes mutually authenticated, strongly encrypted comms w/pilot (e.g. to command exit from emergency UVR)

Steps:
(1) RID Bluetooth Broadcast
(2) DNS Query
(3) HIP Resource Record
(4) XACML Authorized RDAP Query
(5) Operator Personally Identifiable Information (PII)
(6,7) HIP sets up IPsec ESP Bound End-to-End Tunnel (BEET)

Internet

(7)

(6)

UA1
Pilot / Operator

UA2
Pilot / Operator

Pilot/Operator gets alert in web browser, accepts SIP VoIP call from Observer

(2) (3)

(5)

(4)

Public Registry

DNS

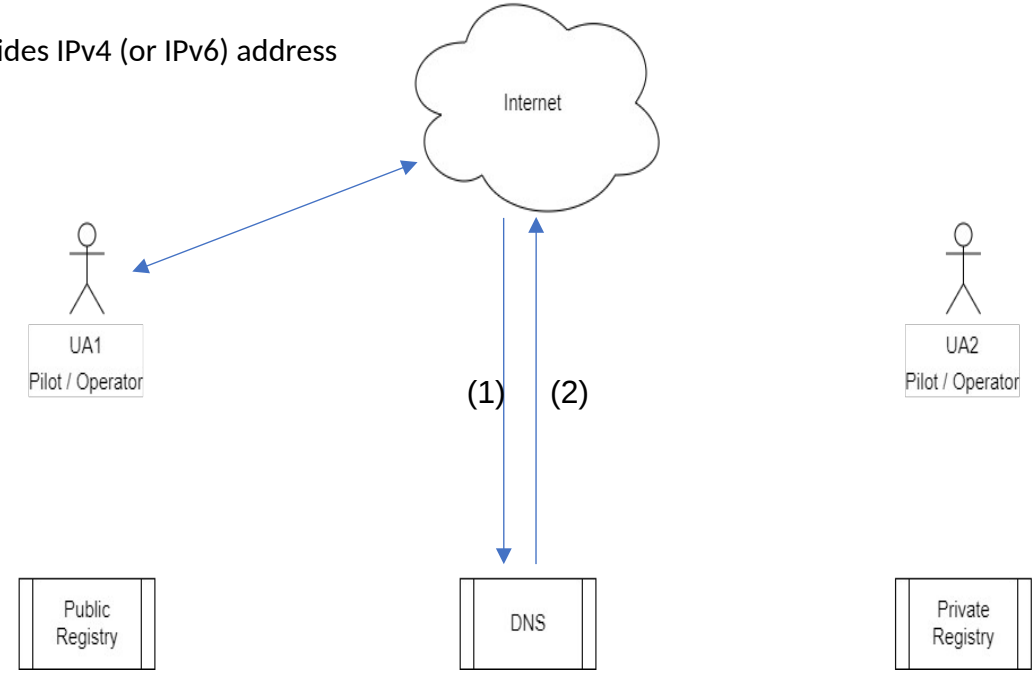
Private Registry

DNS: lookup of *locator* (IP address)

Steps:

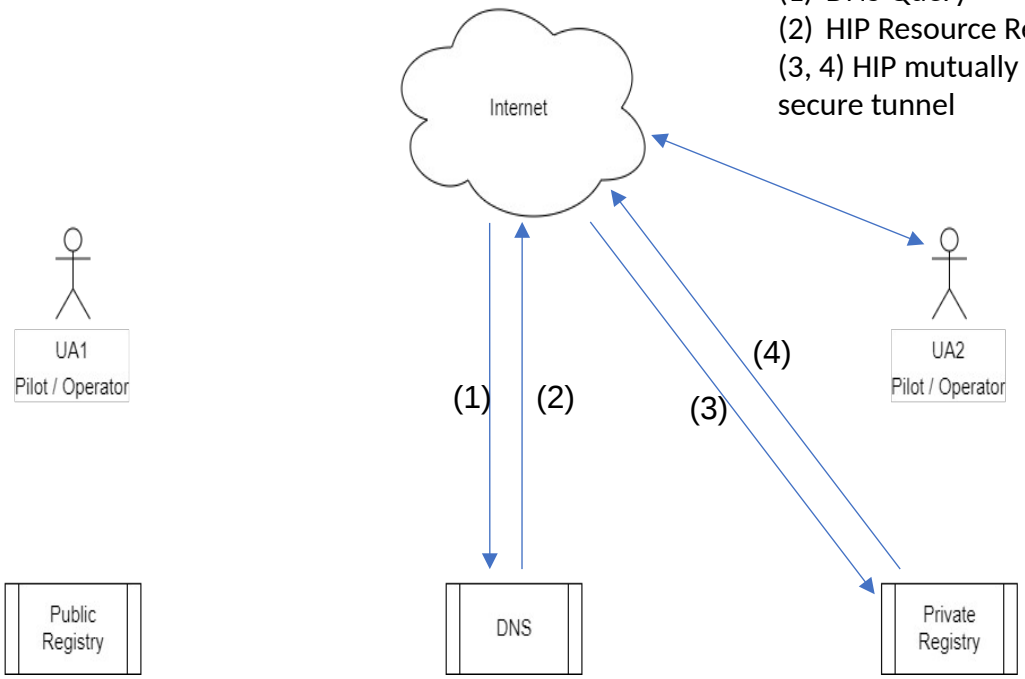
(1) DNS Query

(2) A (or AAAA) RR provides IPv4 (or IPv6) address of Registry



DNS + HIP: lookup & use of locator & *identifier* ([Hierarchical] Host Identity [Tag])

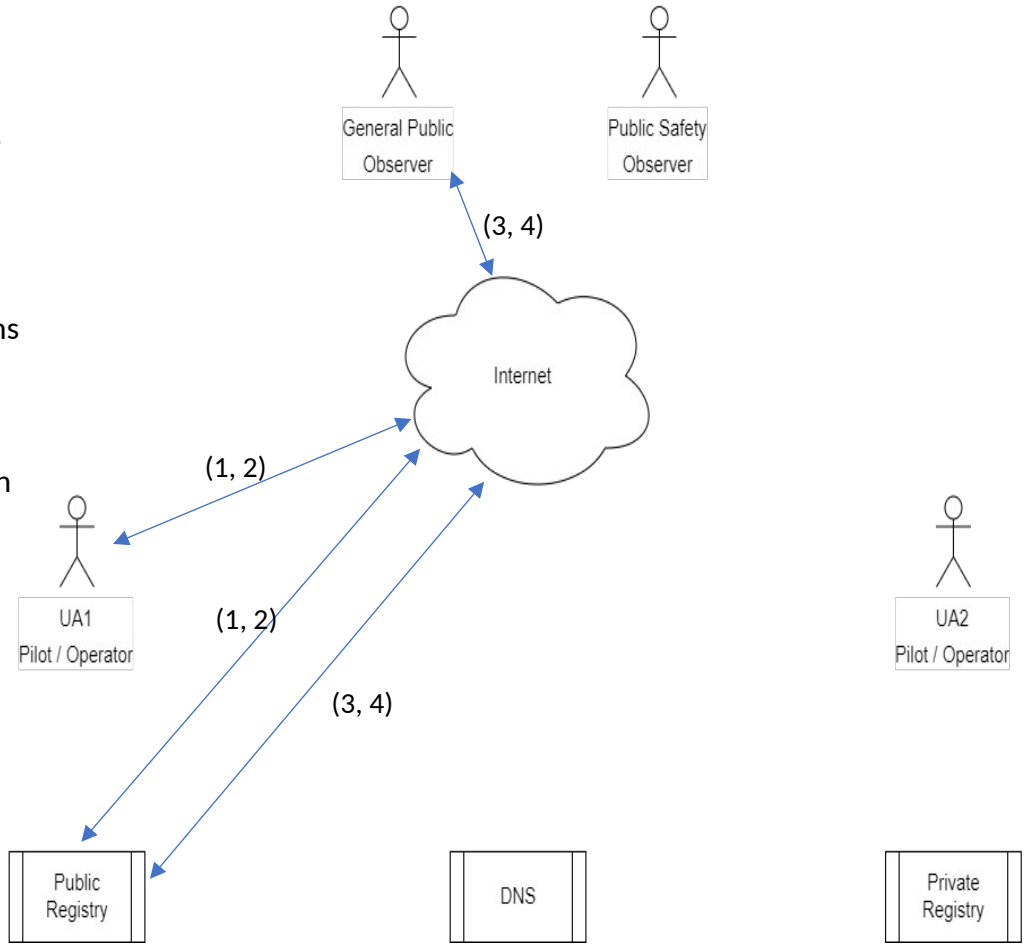
Steps:
(1) DNS Query
(2) HIP Resource Record
(3, 4) HIP mutually authenticates + optionally sets up secure tunnel



whois: public registry lookup

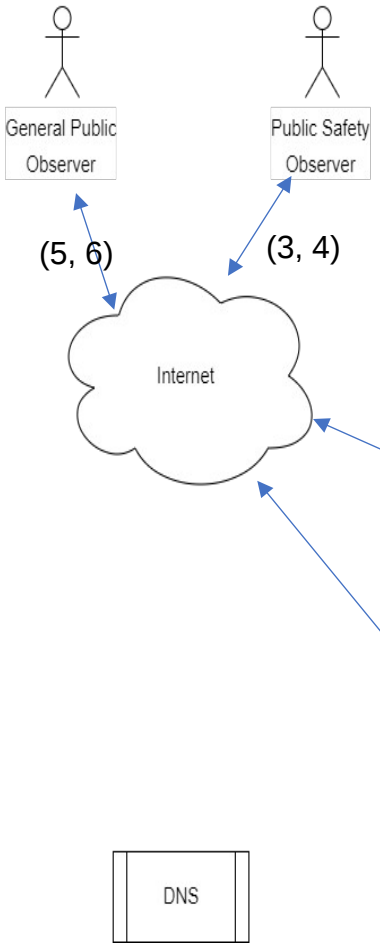
Steps:
(1, 2) Operator registers domain name (e.g. adamsdrone.com)

(3, 4) Whois adamsdrone.com returns lots of PII to anyone (unless it is a private registration, which typically requires human contact & a search warrant)



RDAP/XACML: access controlled registry lookup

(5, 6) Observer w/credentials not satisfying access control policy of this registration gets denied PII of Operator [XACML Request + Denial]

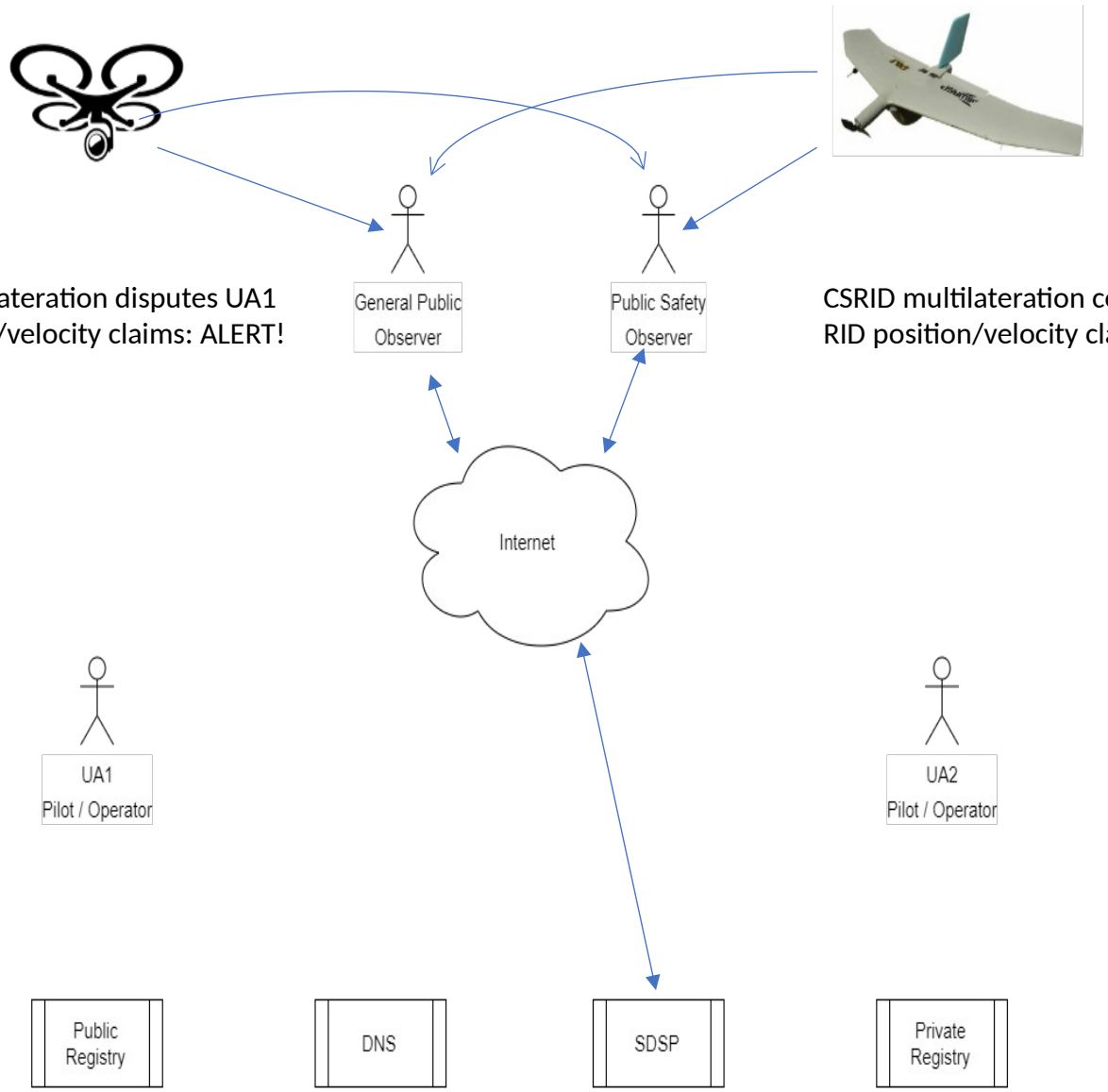


(3, 4) Observer w/credentials satisfying access control policy looks up PII of Operator [XACML Authorized RDAP Query + Response]

(1, 2) Operator privately registers HHIT based domain name

Leverages protocols, infrastructure and business models of Internet domain name registration

Crowd Sourced RID (CSRID):
Broadcast RID ⎵ Network RID Gateway & Multilateration



(tm-rid) Interim 2010 FEB 06 THU: Requirements Discussion

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com

Substantive content additions/deletions/modifications or editorial comments?
https://datatracker.ietf.org/doc/draft-card-tmrid-uas-arch (not there yet, but soon!)