Trustworthy Multipurpose Remote Identification (tm-rid) Interim Webex 2010 FEB 06 THU: Background & Requirements

Stu Card, Adam Wiethuechter

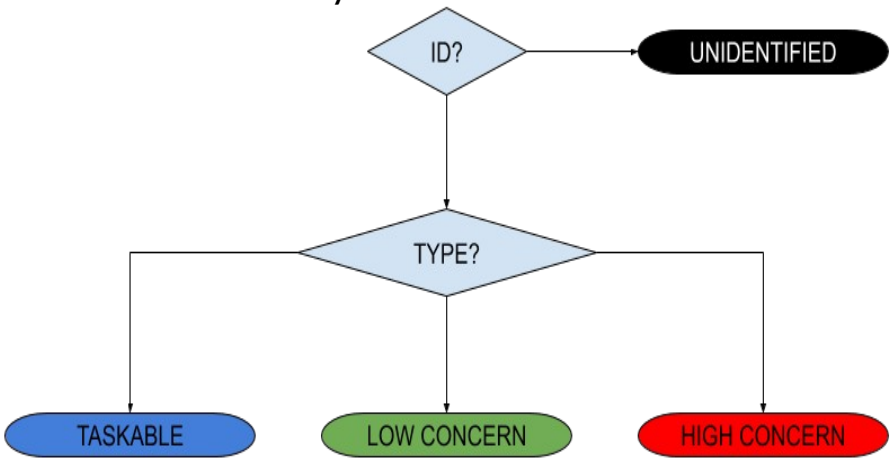
Progress & Next Steps to add strong authentication techniques to identify physically nearby objects

Unmanned Aircraft System (UAS) Remote Identification (RID): Background

- Need means to identify nearby observed Unmanned Aircraft (UA)
  complicated by small size, hi speed (relative to size), remote operation, autonomy…
- Urgent
  - EASA (EU) regulations already issued, become effective June 15 (check date)
  - FAA (US) Notice of Proposed Rule Making (NPRM) comment period ends March 01
  - Manufacturers will build to regs, locking in {good|bad} design for at least life of aircraft!
- ASTM F38.02 WK65041 new standard: OpenDroneID messages / multi transports
  - Network: from UAS (e.g. via LTE) or proxy (e.g. operator phone) via Internet to local observer phone
  - Broadcast: Bluetooth 4 / 5 & WiFi beacons (short packets!) direct to observer phone [w/o Internet]
- Initial ASTM standard falls short in making UAS RID information *immediately actionable*:
  - trustworthy
  - show whether operator is trusted, even if observer lacks Internet
  - enable instant O2P2 & M2M secure comms, if endpoints have Internet
- Aviators familiar w/radio comms, not networking; IETF could help
  - leverage existing Internet services/infrastructure/protocols (e.g. WHOIS/RDAP, EPP, DNS, HIP)
  - strengthen authentication, balance operator privacy w/genuine Need To Know
  - generalize to support V2X, self-separation, collision avoidance
- (UA physical location : UA ID) ~ (host logical location (IP) : host ID)
  we have prototyped & flown a HIP based extension to OpenDroneID @NY UAS Test Site

UAS RID is Critical for UAS Traffic Management (UTM)

- Observing UA at a particular location, need to learn WHO (ID)
  - Using that ID, observer can look up WHAT, WHY, “friendly”, etc.
- Relevant for many entities for various reasons
  - ATC, Public Safety Officials, Homeland Security, General Public, Private Security Personnel, Drone Operators…
  - Vehicle to Infrastructure (V2I) + Vehicle to Vehicle (V2V) = V2X, C2, coordinated separation / collision avoidance, payload mission…
- Trust begins with identity
  - So identity needs to be trustworthy!



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

ASTM F38.02 WK65041 UAS RID

- Focused on message formatting and performance in Remote ID
- Broadcast RID
  - Direct from UA to observer device (data link, not network)
  - Bluetooth 4/5 & Wi-Fi w/Neighbor Awareness Networking (NAN)
    - “selected for compatibility with commonly carried hand-held devices”
    - BT4 Advertisement beacon payload limit of 25 bytes (24 usable)
  - Broadcast always while in flight
- Network RID
  - Typically LTE
  - Net-RID Service Provider (NETSP)
    - UTM USS to which the UAS is subscribed
    - Receives, stores & answers NETDP queries re: UAS ID, location, etc.
  - Net-RID Display Providers (NETDP)
    - Aggregates info from multi NETSP
    - Provides picture of airspace volume in response to client queries
    - May or may not itself be a USS
  - Uses JSON and RestAPI to send information back and forth
- Security methods punted to implementors, only framing specified

FAA NPRM

- Standard Remote ID
  - Both Broadcast RID & Network RID required
  - Both GCS (pilot) & UA locations transmitted
- Limited Remote ID
  - Small UA operating V-LOS within 400’ of pilot
  - Network RID only (Broadcast *prohibited*)
  - GCS location only (not UA)
- Two ID types
  - 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)

FAA UAS Traffic Management (UTM) Pilot Project 2 (UPP2) Architecture

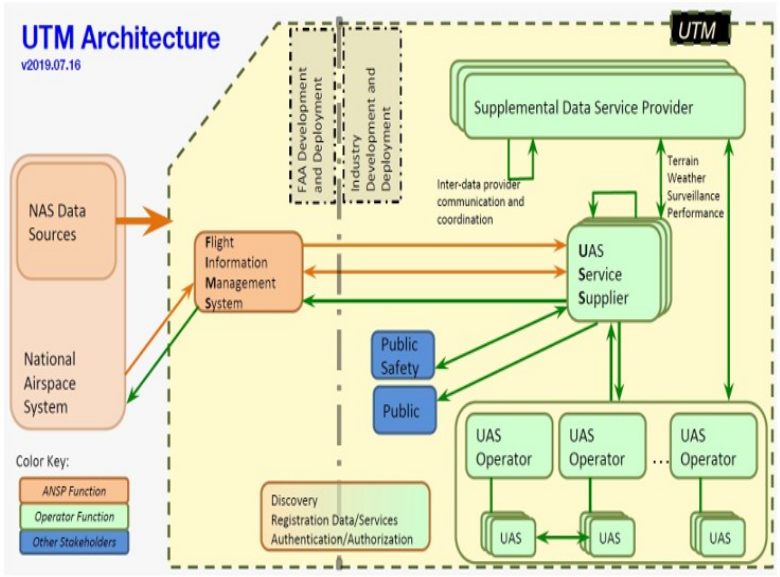


Figure 4-1: Notional Architecture

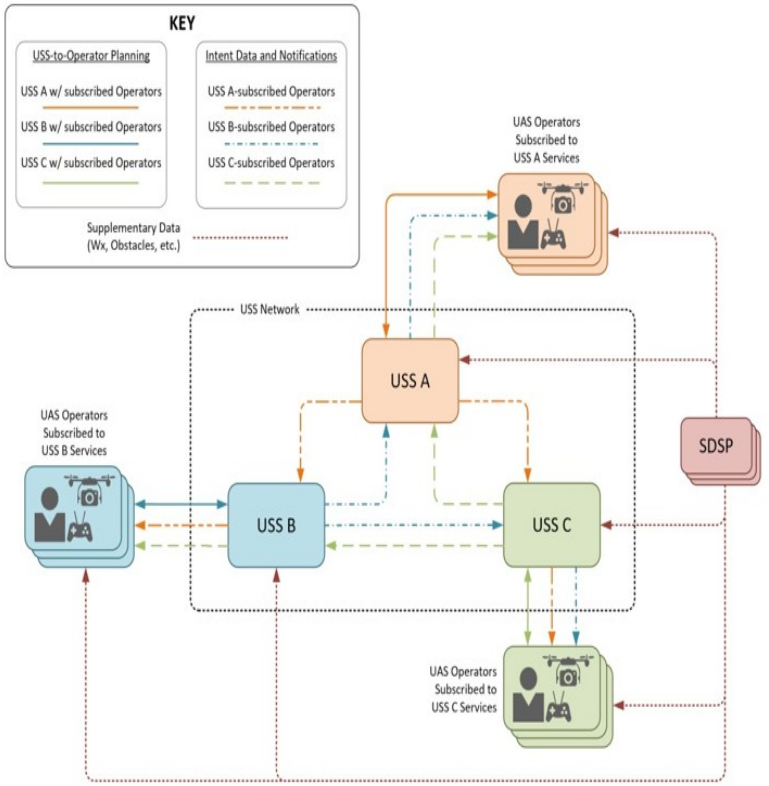


Figure 6-1: Notional High-Density Operations in UTM

UPP2 Use Case 4

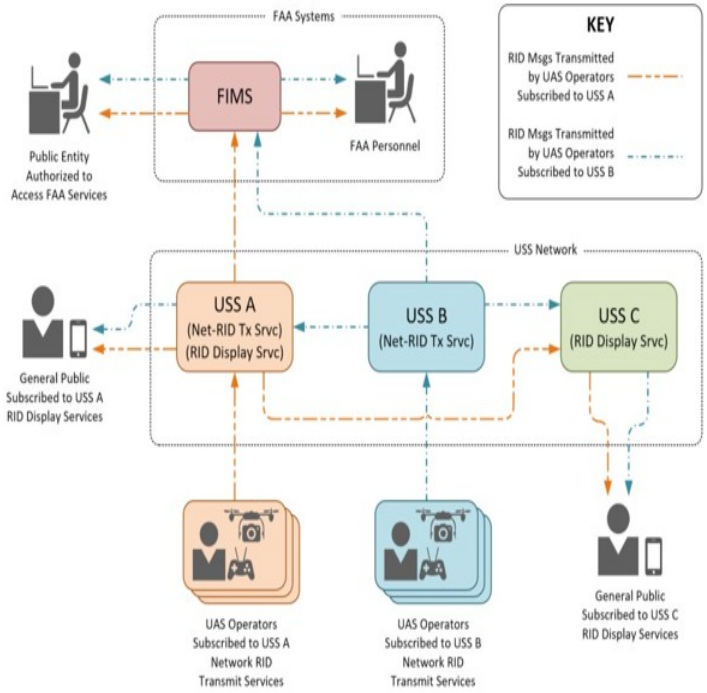


Figure 9-1: Remote ID Message Transmission via Network Publication Flow

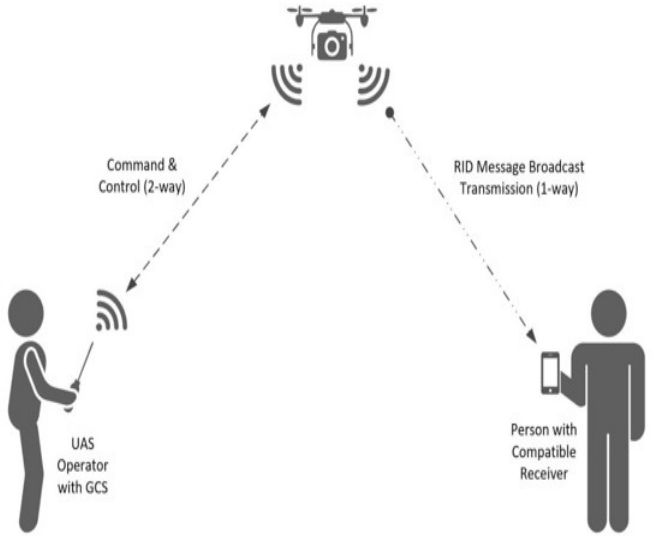


Figure 9-2: Remote ID Message Transmission via Broadcast

AXE UPP2 Use Case 5

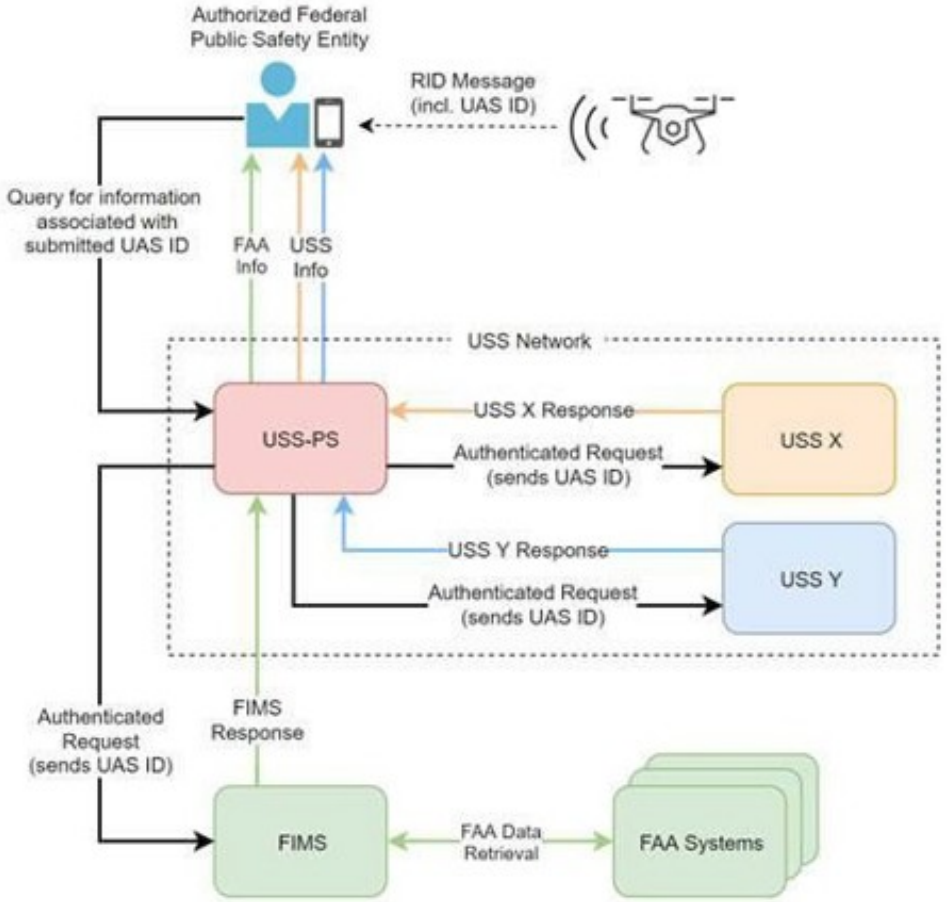


Figure 10-1: Direct Query to FAA and USS Network

Difference between ASTM & NPRM

- Overall they are intended to complement each other
  - FAA rules mandate what must be done & performance requirements
  - ASTM specifies an industry consensus technical means of compliance
- Slightly different terminology
  - NPRM “Remote ID USS” == ASTM “Net-RID Service Provider”
  - NPRM “Session ID” == ASTM “UTM Assigned ID”
- Message elements
  - NPRM requires GCS location (longitude, latitude, pressure altitude)
    - ASTM has most of these in optional messages (that can be required by CAA)
- NPRM baseline is Network RID, ASTM baseline is Broadcast RID
  - NPRM getting push-back on this esp. as EU allows Broadcast
  - One or both will change
- Integrity, security & privacy
  - NPRM mandates error correction & “cybersecurity”
  - ASTM specified only framing of authentication data, not auth methods
  - Both give a nod to the idea that UAS operator privacy must be maintained if not forfeited by the UAS operator through clueless, careless or criminal actions

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

1. 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.

2. 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) 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-reqs