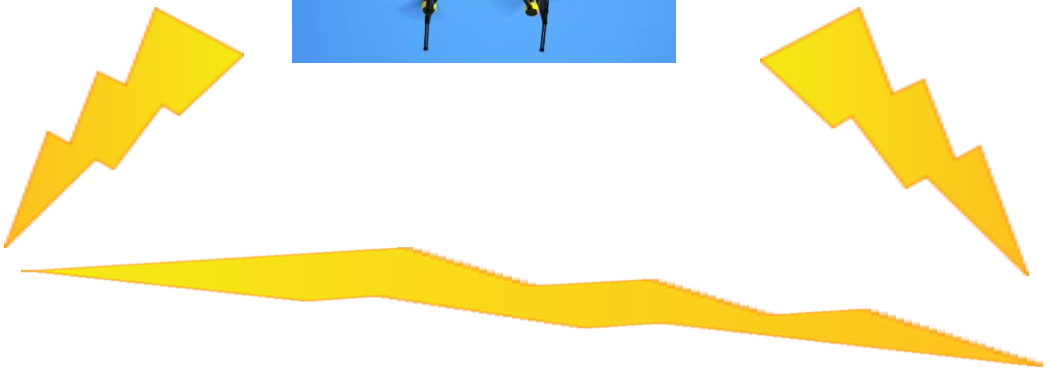


shutterstock · 148735430

IETF 107

Drone Remote Identification Protocol (DRIP) WG

formerly Trustworthy Multipurpose Remote Identification (TM-RID) BoF

Background/Context & Use Cases ⇒ draft-card-drip-reqs

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com

Identify & track [cooperative] [dangerous] [mobile] physical objects

Some acronyms (sorry, mostly use case related)

- UA: Unmanned Aircraft (“drone”)
- GCS: Ground Control Station (pilot uses to operate UA)
- UAS: Unmanned Aircraft System (UA + GCS)

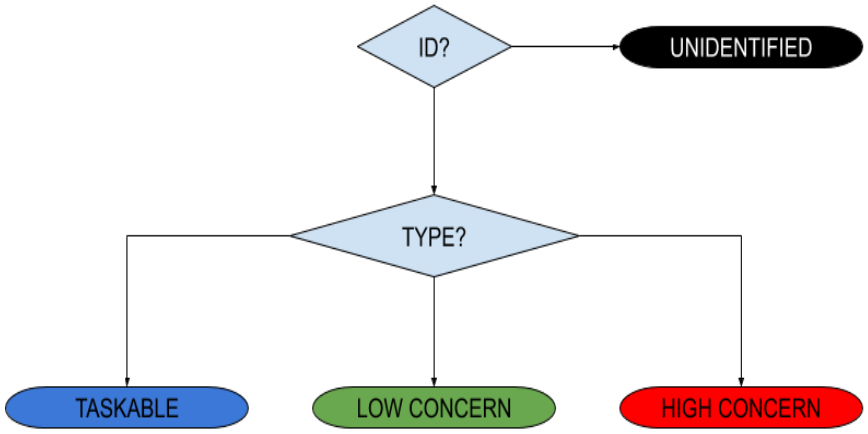
- USS: UAS Service Supplier
- SDSP: Supplemental Data Service Provider
- UTM: UAS Traffic Management (distributed system inc. many USS, SDSP, etc., hoped to scale better than humans using voice comms for Air Traffic Control [ATC])
- UVR: UAS Volume Reservation (temporary no-fly zone for most operators)
- UAS RID: UAS Remote Identification [&Tracking]

- SDO: Standards Development Organization
- ASTM: ASTM International, formerly American Society for Testing and Materials (SDO)
- CTA: Consumer Technology Association (SDO)
- CAA: Civil Aviation Authority (regulator)
- EASA: European Union Aviation Safety Agency (CAA)
- FAA: United States Federal Aviation Administration (CAA)
- NPRM: Notice of Proposed Rule Making

- PII: Personally Identifiable Information (more generally, information to be kept private)
- AAA: Attestation, Authentication, Authorization, Access Control, Accounting, Attribution, Audit

UAS Remote ID is Critical for 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
  - Air Traffic Control (ATC), Public Safety Officials, Homeland Security, General Public, Private Security Personnel, Drone Operators...
  - Vehicle to Infrastructure (V2I) + Vehicle to Vehicle (V2V) = V2X
  - Command & Control (C2) of UA
  - coordinated separation / collision avoidance / Detect And Avoid (DAA)
  - payload mission…
- Trust begins with identity
  - So identity needs to be trustworthy!



Complex, rapidly evolving environment…

- Constituent systems/technologies in loosely coupled development – RID, DAA, V2X, Comm Protocols/Radios/Spectrum…
- UTM is a moving target… but we still need to hit it…
  - 2 architectures still being debated – federated *vs* global
  - USS Discovery & Synch. Service – most current USS prototypes don't yet interoperate
  - SDSPs – no standardized interface
  - Flight Priority/Deconfliction – not well defined
  - Government / Public Safety Access & Priority – required, but unspecified
  - Operator & UAS registries/databases – unaddressed
  - Information Sharing – InterUSS protocol defined, but who can share what with whom…
- Cybersecurity, Access Control & Trust Frameworks – still being defined
  - International Civil Aviation Organization (ICAO) Trust Framework (IATF) / Global Resilient Aviation Interoperable Network (GRAIN)
- Urban/Advanced Air Mobility (UAM, AAM: think robotic air taxi) requirements – just beginning to be considered…

FAA UTM Pilot Project 2 (UPP2) Architecture

(DRIP must fit here as well as in EU equivalent)

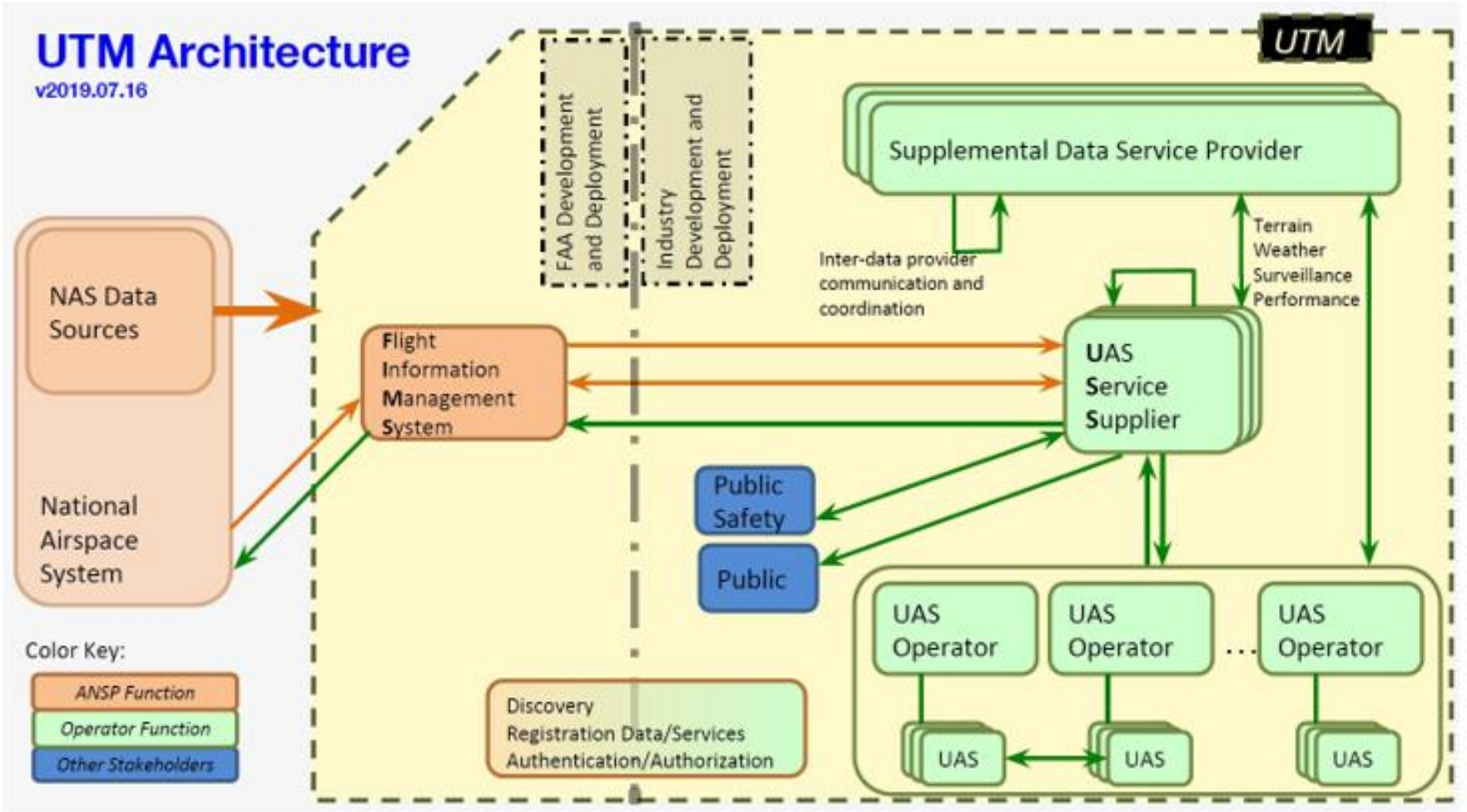


Figure 4-1: Notional Architecture

ASTM F3411-19 Standard Specification for Remote ID and Tracking (1st version from F38.02 WK65041)

- Focused on message formatting & 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 Provider (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 / RestAPI to exchange information
- Security methods punted to implementors, only framing specified

UPP2 Use Case 4

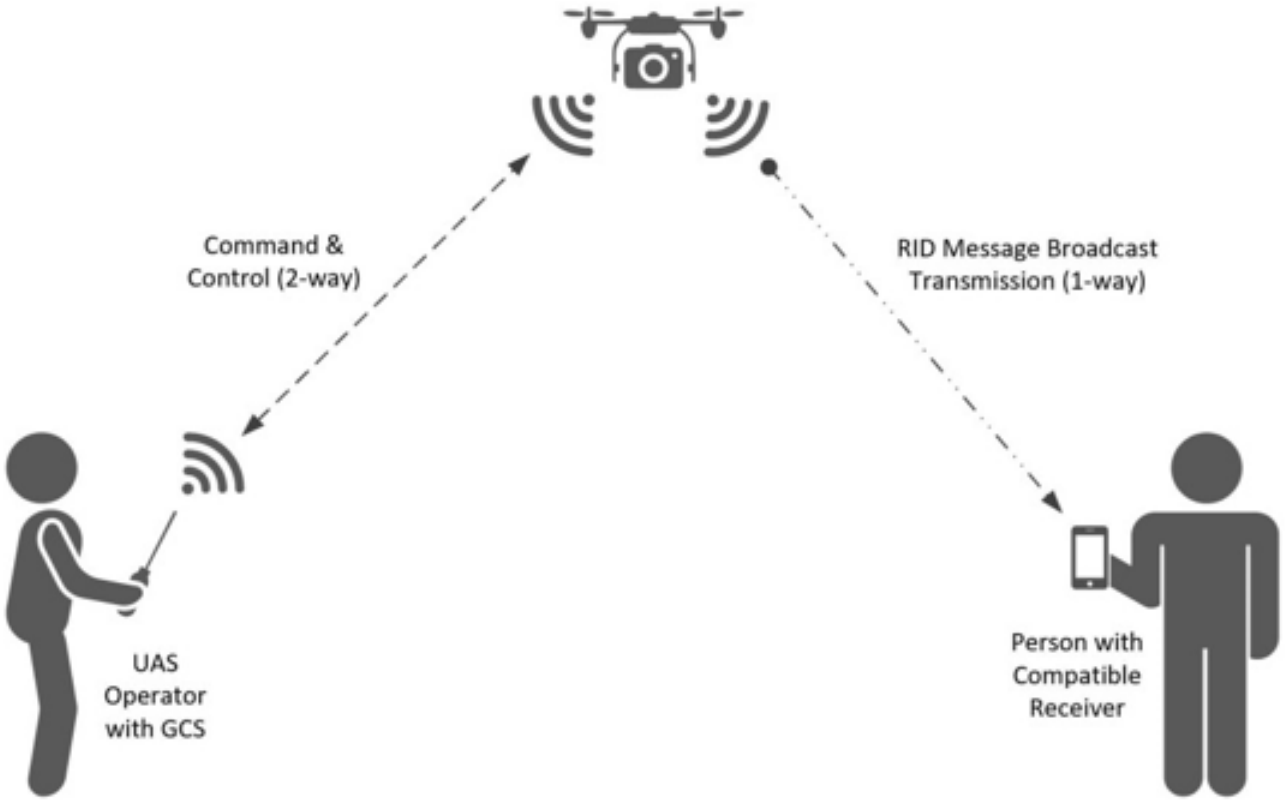


Figure 9-2: Remote ID Message Transmission via Broadcast

UPP2 Use Case 4

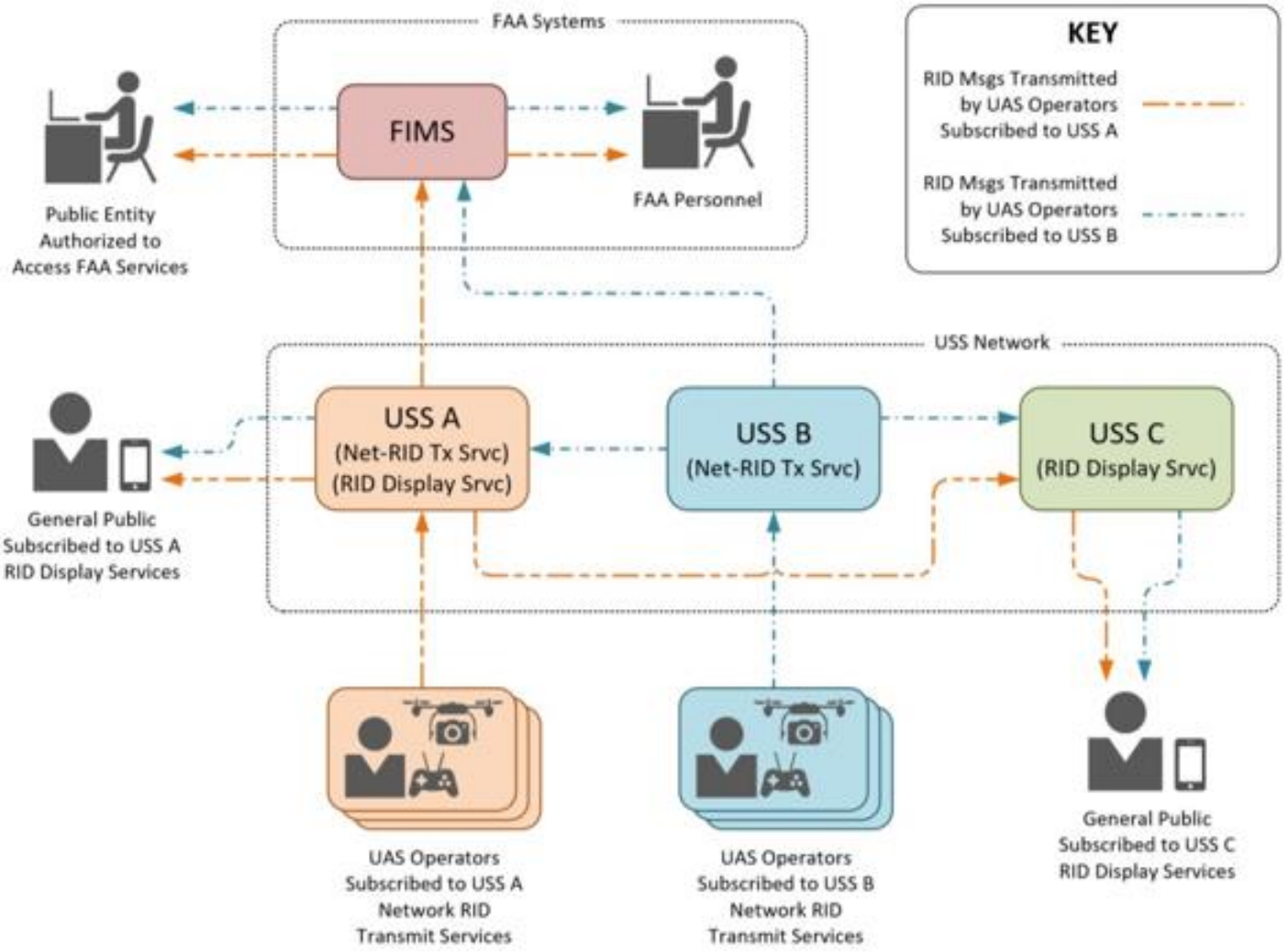


Figure 9-1: Remote ID Message Transmission via Network Publication Flow

Regulations *vs* Industry Consensus Standards

- Overall they are intended to complement each other
  - EASA, FAA, *et al* rules mandate what must be done & performance requirements
  - ASTM *et al* technical specifications detail one or more means that might be used
  - Regulators may designate industry standards as “accepted means of compliance”, relieving operators who buy gear whose manufacturers assert they follow such standards from each having to prove their own compliance
- Slightly different terminology, e.g.
  - FAA NPRM “Remote ID USS” == ASTM “Net-RID Service Provider”
  - FAA NPRM “Session ID” which could be an ASTM “UTM Assigned ID” == UUIDv4
- Acceptability of tech spec options vary per regulators, e.g. ASTM F3411-19 UAS ID Types
  - Type 1: Manufacturer assigned Hardware Serial # per ANSI/CTA-1063-A: required by EASA; allowed by FAA
  - Type 2: CAA assigned ID (e.g. aircraft registration number): not allowed by either
  - Type 3: not allowed by EASA; “randomly-generated alphanumeric code that is used only for one flight”) Session ID encouraged by FAA (p. 21, NPRM)
- Stakeholder needs recognized by regulators will influence standards that manufacturers will follow in producing aircraft & ground systems that will remain in use for many years

Regulations & Means of Compliance: Industry "Consensus" Standards

	ASTM Broadcast RID Bluetooth/WiFi direct from UA	ASTM Network RID Internet from UAS (UA or GCS)
EASA Europe likely to influence rest of world outside N. America	**Pilot/GCS & UA locations** **UA serial # (manufacturer assigned)**	**N/A**
FAA NPRM Limited RID Small UA, Visual Line of Sight (V-LOS) within 400' of pilot	**prohibited**	**Pilot/GCS location only** **UA serial # or 1-time session ID**
FAA NPRM Standard RID	**Pilot/GCS & UA locations** **UA serial # or 1-time session ID**	**Pilot/GCS & UA locations** **UA serial # or 1-time session ID**

- NPRM says RID is an enabler of DAA, V2X, etc.;
  but ASTM F38.02 says RID is just RID.
- NPRM calls for error correction;
  but ASTM F3411-19 does not specify any.
- NPRM calls for cybersecurity to protect integrity & authenticity;
  but ASTM F3411-19 specifies only the framing of authentication data.
- Everyone says protect operator privacy;
  but pilot/GCS location is broadcast in the clear &
  no one specifies how to protect PII in registries…

UPP2 Use Case 5

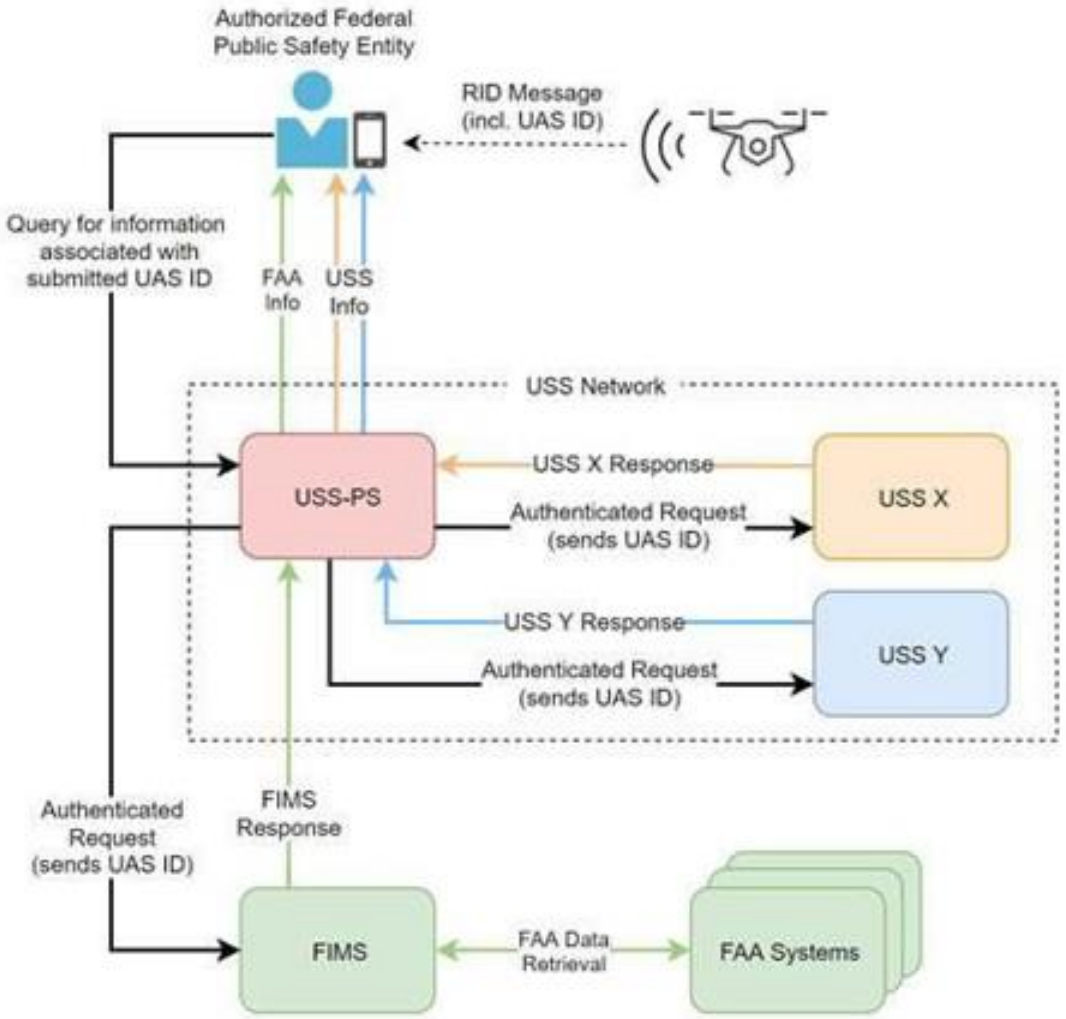


Figure 10-1: Direct Query to FAA and USS Network

1. DRIP General Requirements

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 & 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. DRIP UAS Identifier Requirements

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 DRIP 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 DRIP WG 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 DRIP WG 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.

DRIP Intro Recap

- Important: 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 July 01
  - FAA (US) NPRM comment period ended March 02, final rules expected in 1 year
  - Manufacturers will build to regs, locking in {good|bad} design for at least life of aircraft!
- Initial ASTM F3411-19 standard falls short in making information *immediately actionable*:
  - trustworthy
  - show whether operator is trusted, even if observer lacks Internet connectivity
  - enable instant Observer to Pilot & M2M secure comms, if endpoints have IP connectivity
- Aviators familiar w/radio comms, not networking; IETF can help
  - leverage existing Internet businesses/services/infrastructure/protocols (e.g. WHOIS/RDAP, EPP, DNS)
  - strengthen authentication, balance operator privacy w/genuine Need To Know
  - generalize to support V2X, C2, self-separation, collision avoidance, mission…
  - extend w/Broadcast->Network gateways & multilateration for tracks independent of self-reports
- (UA physical location : UA ID) ~ (host logical location (IP) : host ID)
  we have prototyped & flown a HIP based extension to OpenDroneID at the NY UAS Test Site

➢ **We need your help: reviewers, authors, implementers, testers…**