Drone Remote Identification Protocol (DRIP)

tm-rid@ietf.org (Trustworthy Multipurpose Remote ID)

https://datatracker.ietf.org/wg/drip

interim meeting 2020 MAY 27

draft-ietf-drip-reqs-01 & -arch-01

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com
shuaiizhao@tencent.com
Andrei Gurtov gurtov@acm.org

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

Summary of Changes since APR 22

- Consolidated definitions in –reqs
- Removed much of the redundancy between –reqs & –arch
- Numbered the previously un-numbered requirements
- Broke out registries requirements as a new group
- Incrementally harmonized w/EASA, ICAO
- Updated references to other drafts (Bob has been busy!)
- Added discussion/limitations section to –reqs (thanks Andrei!)
- Added Broadcast PII privacy section PII to –arch
- Added ASCII art to both drafts (thanks Andrei!)
- Added authors ☺
- Addressed comments from Amelia Andersdotter, Mohamed Boucadair, Toerless Eckert, Susan Hares, Mika Jarvenpaa, Daniel Migault, Saulo Da Silva & Shuai Zhao (my apologies if I failed to list you, thanks all!)

Drone Remote Identification Protocol (DRIP)

tm-rid@ietf.org (Trustworthy Multipurpose Remote ID)

https://datatracker.ietf.org/wg/drip

interim meeting 2020 MAY 27

draft-ietf-drip-**reqs-01** & -arch-01

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com
shuaiizhao@tencent.com
Andrei Gurtov gurtov@acm.org

Not only the UA but also the regs & external standards are moving targets.

DRIP General Requirements

- **GEN-1 Provable Ownership**

DRIP MUST enable verification that the UAS ID asserted in the Basic ID message is that of the actual current sender of the message (i.e. the message is not a replay attack or other spoof, authenticating e.g. by verifying an asymmetric cryptographic signature using a sender provided public key from which the asserted ID can be at least partially derived), even on an observer device lacking Internet connectivity at the time of observation.

- **GEN-2 Provable Binding**

DRIP MUST enable binding all other F3411 messages from the same actual current sender to the UAS ID asserted in the Basic ID message.

- **GEN-3 Provable Registration**

DRIP MUST enable verification that the UAS ID is in a registry and identification of which one, even on an observer device lacking Internet connectivity at the time of observation; with UAS ID Type 3, the same sender may have multiple IDs, potentially in different registries, but each ID must clearly indicate in which registry it can be found.

DRIP General Requirements

- **GEN-4 Readability**

DRIP MUST enable information (regulation required elements, whether sent via UAS RID or looked up in registries) to be read and utilized by both humans and software.

- **GEN-5 Gateway**

DRIP MUST enable Broadcast RID -> Network RID gateways to stamp messages with precise date/time received and receiver location, then relay them to a network service (e.g. SDSP or distributed ledger), to support three objectives: mark up a RID message with where and when it was actually received (which may agree or disagree with the self-report in the set of messages); defend against reply attacks; and support optional SDSP services such as multilateration (to complement UAS position self-reports with independent measurements).

- **GEN-6 Finger (placeholder name)**

DRIP MUST MUST enable dynamically establishing, with AAA, per policy, E2E strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including at least the remote pilot and USS.

DRIP General Requirements

- **GEN-7 QoS**

DRIP MUST enable policy based specification of performance and reliability parameters, such as maximum message transmission intervals and delivery latencies.

- **GEN-8 Mobility**

DRIP MUST support physical and logical mobility of UA, GCS and Observers. DRIP SHOULD support mobility of all participating nodes. (UA, GCS, Observers, Net-RID SP, Net-RID DP, Private Registry, SDSP).

- **GEN-9 Multihoming**

DRIP MUST support multihoming of UA, for make-before-break smooth handoff and resiliency against path/link failure. DRIP SHOULD support multihoming of essentially all participating nodes.

- **GEN-10 Multicast**

DRIP SHOULD support multicast for efficient and flexible publish-subscribe notifications, e.g. of UAS reporting positions in designated sensitive airspace volumes.

- **GEN-11 Management**

DRIP SHOULD support monitoring of the health and coverage of Broadcast and Network RID services.

DRIP Identifier Requirements

- **ID-1 Length**

The DRIP [UAS] entity [remote] identifier must be no longer than 20 bytes (per [F3411-19] to fit in a Bluetooth 4 advertisement payload).

- **ID-2 Registry ID**

The DRIP identifier MUST be sufficient to identify a registry in which the [UAS] entity identified therewith is listed.

- **ID-3 Entity ID**

The DRIP identifier MUST be sufficient to enable lookup of other data associated with the [UAS] entity identified therewith in that registry.

- **ID-4 Uniqueness**

The DRIP identifier MUST be unique within a to-be-defined scope.

- **ID-5 Non-spoofability**

The DRIP identifier MUST be non-spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID).

DRIP Identifier Requirements

- **ID-6 Unlinkability**

A DRIP UAS ID MUST NOT facilitate adversarial correlation over multiple UAS operations; this may be accomplished e.g. by limiting each identifier to a single use, but if so, the UAS ID MUST support well-defined scalable timely registration methods).

- **Unnumbered explanatory text**

Whether a UAS ID is generated by the operator, GCS, UA, USS or registry, or some collaboration thereamong, is unspecified; however, there must be agreement on the UAS ID among these entities.

DRIP Privacy Requirements

- **PRIV-1 Confidential Handling**

DRIP MUST enable confidential handling of private information (i.e. any and all information designated by neither cognizant authority nor the information owner as public, e.g. personal data).

- **PRIV-2 Encrypted Transport**

DRIP MUST enable selective strong encryption of private data in motion in such a manner that only authorized actors can recover it. If transport is via IP, then encryption MUST be end-to-end, at or above the IP layer.

- **PRIV-3 Encrypted Storage**

DRIP SHOULD enable selective strong encryption of private data at rest in such a manner that only authorized actors can recover it.

- **Unnumbered explanatory text**

As satisfying these requirements may require that authorized actors have connectivity to third parties, e.g., Internet to a Remote ID USS, to enable decryption, and such connectivity cannot be assured, DRIP SHOULD provide automatic fallback to plaintext transmission of safety-critical information when necessary.

DRIP Registries Requirements

- **REG-1 Public Lookup**

DRIP MUST enable lookup, from the UAS ID, of information designated by cognizant authority as public.

- **REG-2 Private Lookup**

DRIP MUST enable lookup, with AAA, per policy, of private information (i.e. any and all information in a registry, associated with the UAS ID, that is designated by neither cognizant authority nor the information owner as public).

- **REG-3 Provisioning**

DRIP MUST enable provisioning registries with static information on the UAS and its operator, dynamic information on its current operation within the UTM (including means by which the USS under which the UAS is operating may be contacted for further, typically even more dynamic, information), and Internet direct contact information for services related to the foregoing.

- **REG-4 AAA Policy**

DRIP MUST enable closing the AAA-policy registry loop by governing AAA per registered policies and administering policies only via AAA

Drone Remote Identification Protocol (DRIP)

tm-rid@ietf.org (Trustworthy Multipurpose Remote ID)

https://datatracker.ietf.org/wg/drip

interim meeting 2020 MAY 27

draft-ietf-drip-reqs-01 & **-arch-01**

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com
shuaiizhao@tencent.com
Andrei Gurtov gurtov@acm.org

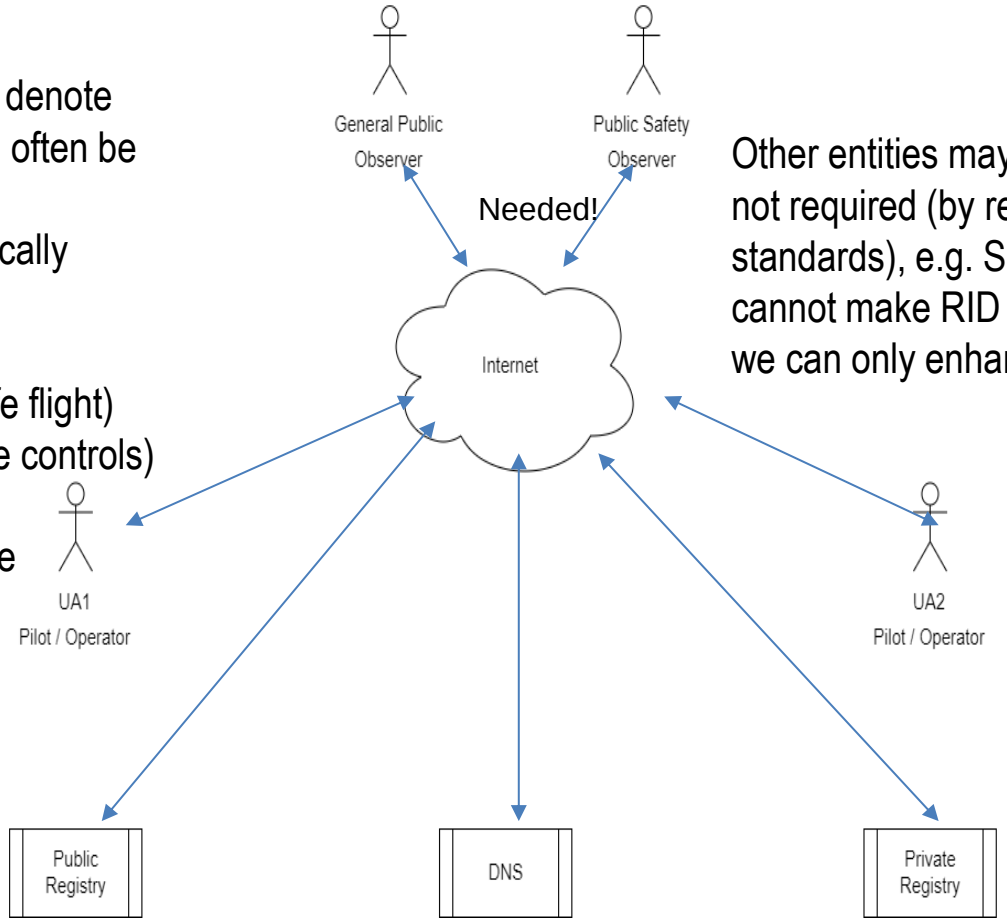
Fit needed functionality within tight UAS RID constraints.

“Reference Architecture”:
really just the cast of characters

UA is Broadcast RID source

By “Pilot/Operator”, we denote several entities that will often be identical or colocated:

- UAS Operator (typically owner or lessee)
- Pilot In Command (responsible for safe flight)
- Remote Pilot (at the controls)
- GCS (the controls)
- Network RID source



Other entities may be in play but are not required (by regulations or external standards), e.g. SDSPs, but we cannot make RID depend on SDSPs, we can only enhance it w/such

By “registry”, we denote several functions that will almost certainly be offered by the same service bureaus:

- UAS Operator registry
- UA registry
- UTM USS
- Net-RID Service Provider
- Net-RID Display Provider

Network RID Data Flow

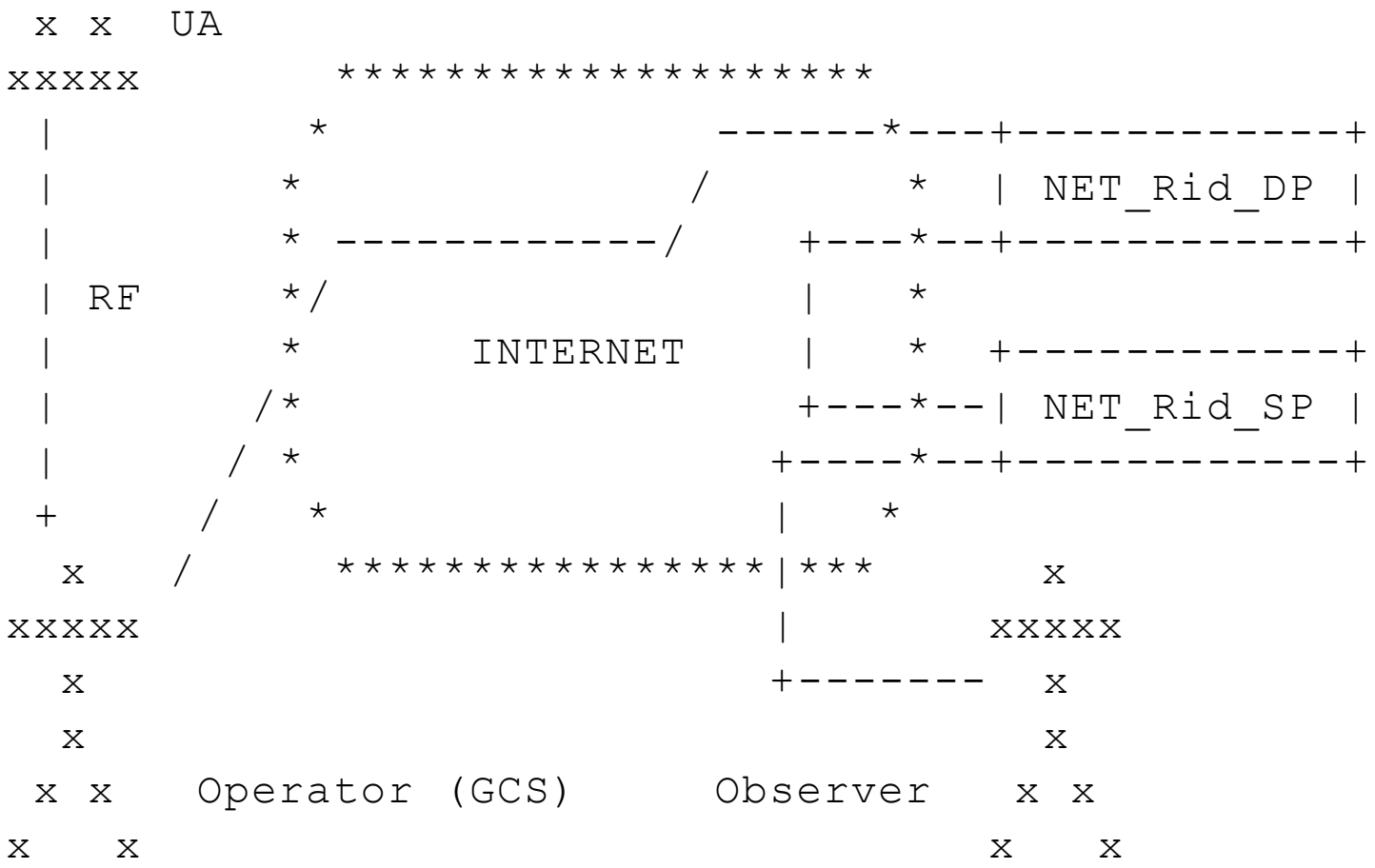


Figure 2

Entities & their Interfaces

Pre-defined – UA + GCS = UAS, Remote Pilot, Pilot in Command, Operator, USS, Net-RID SP, Net-RID DP, Observer (our term) – plus DRIP defined

- Private information registry of Operators & UA (required but unspecified by regs & F3411)
  - **Background:** info required is similar to that required for Internet domain name registration, plus operator credentials, UA hardware gross characteristics (fixed or rotary wing, size), etc.
  - **Proposed approach:** leverage Internet resources by defining a UAS ID as a [pseudo-]domain (if not a FQDN in .aero, then something legit that can be reverse looked up in .ip6.arpa); load UAS ID = Internet domain registries w/Extensible Provisioning Protocol (EPP) as usual; lookup w/Registration Data Access Protocol (RDAP) as usual; add name to DNS as usual
- Public information registry (likewise)
  - **Background:** public info required to be made available by UAS RID is transmitted in plaintext to local observers in Broadcast RID & served to clients by a Net-RID DP in Network RID
  - **Proposed approach:** Observers use DNS to lookup, from the received UAS ID, per RFC 7484, the RDAP server where private info can be requested; put minimal public static human readable UAS RID info in a TXT RR; put direct machine to machine contact info in other RRs
- Optional CS-RID
  - **SDSP:** insert between Net-RID SP DP, look to each like the other; multilaterate Finders' info
  - **Finder:** smartphone app; GNSS position/time-stamp rcvd Broadcast RID msgs; relay to SDSP

Presumed Transactions

- Registrations
  - Registry to CAA
  - Operator to Registry
  - UA to Operator
  - UA via Operator to Registry
- Operations
  - Encrypted PII Broadcast by UA & Decryption by USS-enabled Observer
  - Message Signature by UA & Verification by Observer [w/o Internet]
  - Certificate Broadcast by UA & Verification by Observer [w/o Internet]

    Classification of UAS Trust by Observer [w/o Internet]
  - Lookup of UAS Public Information by Observer w/Internet
  - Lookup of UAS Operator Private Information by Observer w/Internet
  - Observer Initiation of Comms (or other App/IP Flows) w/Remote Pilot
  - Finder relay of Broadcast RID Messages to CS-RID SDSP
  - CS-RID SDSP provision of Fused Data to Net-RID DP

Identifiers

- Background
  - F3411 Basic ID message: 4 bit UAS Type; 4 bit UAS ID Type; 20 B UAS ID; 3 B rsvd
  - F3411 max 10 page Auth message has 224 B (less any error control) for auth data
  - X.509 PKI certificates, even using EdDSA, won't fit in max 10 page message
- Proposed Approach
  - Adopt Host Identity Tag (HIT) from Host Identity Protocol (HIP)
    - 128 bit Overlay Routable Cryptographic Hash Identifier (ORCHID) derived from HI public key
    - ORCHIDs allocated by IANA from IPv6 space, can be used wherever IP address overloaded as ID
  - Extend to provide for a registry hierarchy & Hierarchical HITs (HHITs)
    - First 64 bits ID higher level registry (CAA?) & lower level registry (USS operator?)
    - Last 64 bits derived by sender hashing a [self-generated] HI public key
    - Can be re-derived by any receiver from the HI public key as a sanity check
  - Ask ASTM F38.02 to assign a new UAS ID Type (presumably 4) for HHITs
    or HI can be encoded as Type 1 (ANSI/CTA manufacturer assigned serial #) or Type 3 (UTM UUIDv4)
  - Self-assertion of UAS ID takes 16 B HHIT + 4 B expiry + 64 B EdDSA sig = 84 B
  - Registry certificate on aircraft takes only 200 B
    - Fits in max 10 page msg even if last page used for R-S check bytes sufficient to recover 1 lost page
    - Observers can carry small database of registry public keys to check certs even w/o Internet

Drone Remote Identification Protocol (DRIP)

tm-rid@ietf.org (Trustworthy Multipurpose Remote ID)

https://datatracker.ietf.org/wg/drip

interim meeting 2020 MAY 27

draft-ietf-drip-reqs-01 & -arch-01

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com
shuaiizhao@tencent.com
Andrei Gurtov gurtov@acm.org

in progress

In progress

- Confirm definitions (inc. plural forms) from user community standards esp. ICAO
- Coordinate w/ICAO International Aviation Trust Framework (DI, GRAIN, TRON)
- Focus on registration
- Expand CS-RID coverage?
- Get serious about Operator to Pilot comms?
- Discussion/limitations section?
- Organize set of related drafts
- Add more authors! Get more comments!

Drone Remote Identification Protocol (DRIP)

tm-rid@ietf.org (Trustworthy Multipurpose Remote ID)

https://datatracker.ietf.org/wg/drip

interim meeting 2020 MAY 27

draft-ietf-drip-reqs-01 & -arch-01

stu.card@axenterprize.com 315-725-7002
adam.wiethuechter@axenterprize.com
Robert Moskowitz rgm@labs.htt-consult.com
shuaiizhao@tencent.com
Andrei Gurtov gurtov@acm.org

backup slides

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 & Materials (SDO)
- CTA: Consumer Technology Association (SDO)
- ICAO: International Civil Aviation Organization (SDO-ish)
- 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

FAA's UTM Pilot Project 2 (UPP2) Architecture

(DRIP must fit here & in EU's more ambitious U-space)

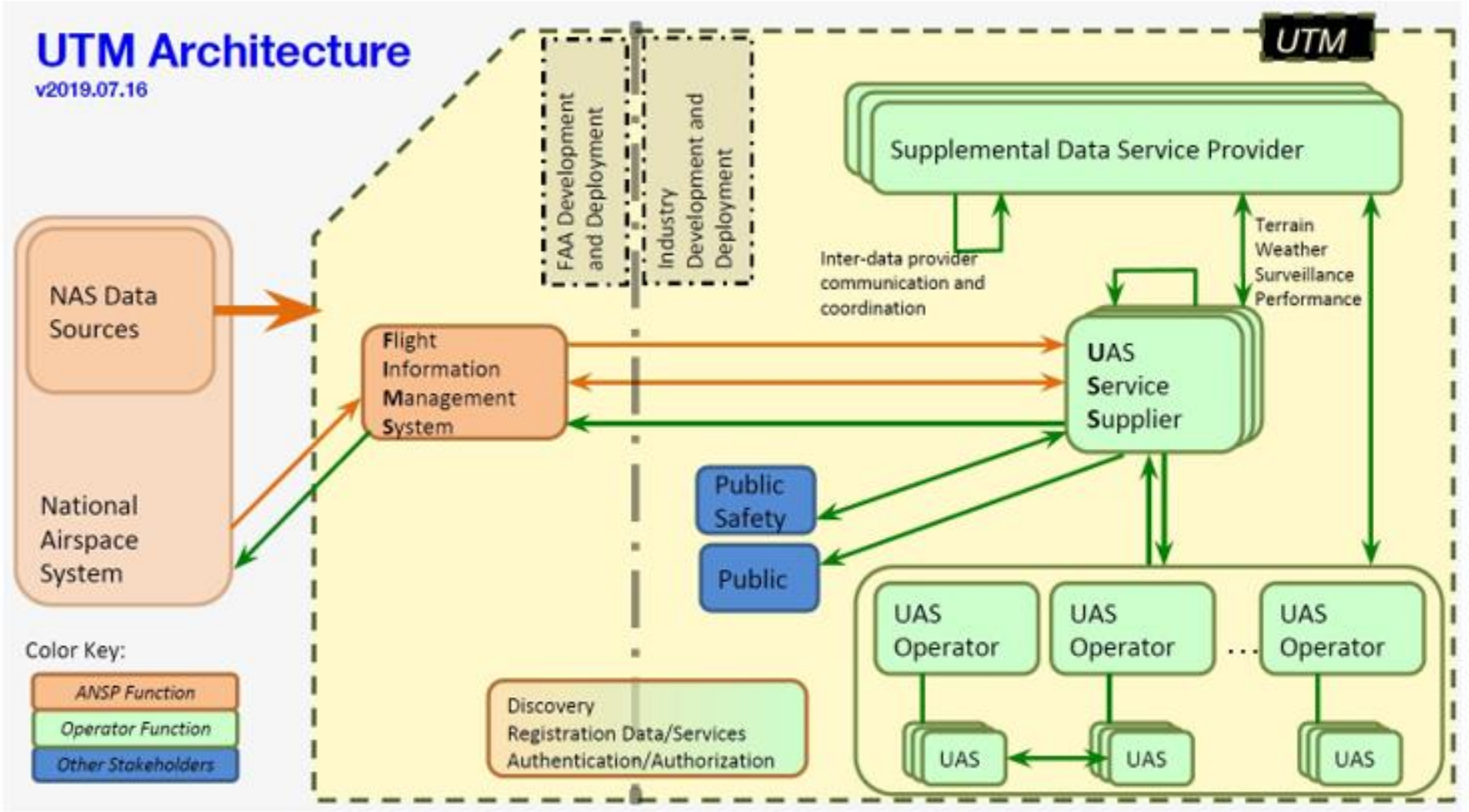


Figure 4-1: Notional Architecture

some but not all of the arrows have interface standards, especially InterUSS

UPP2 Use Case 4

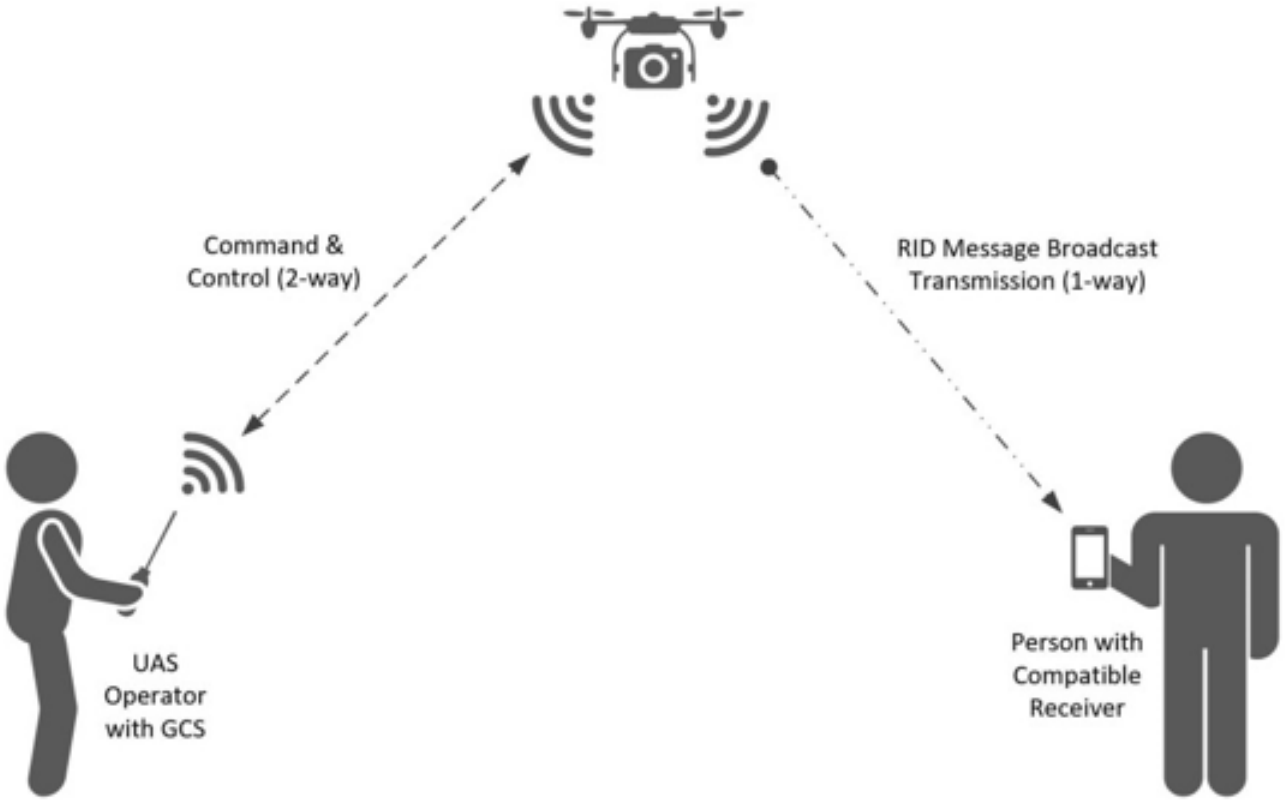


Figure 9-2: Remote ID Message Transmission via Broadcast

UPP2 Use Case 4

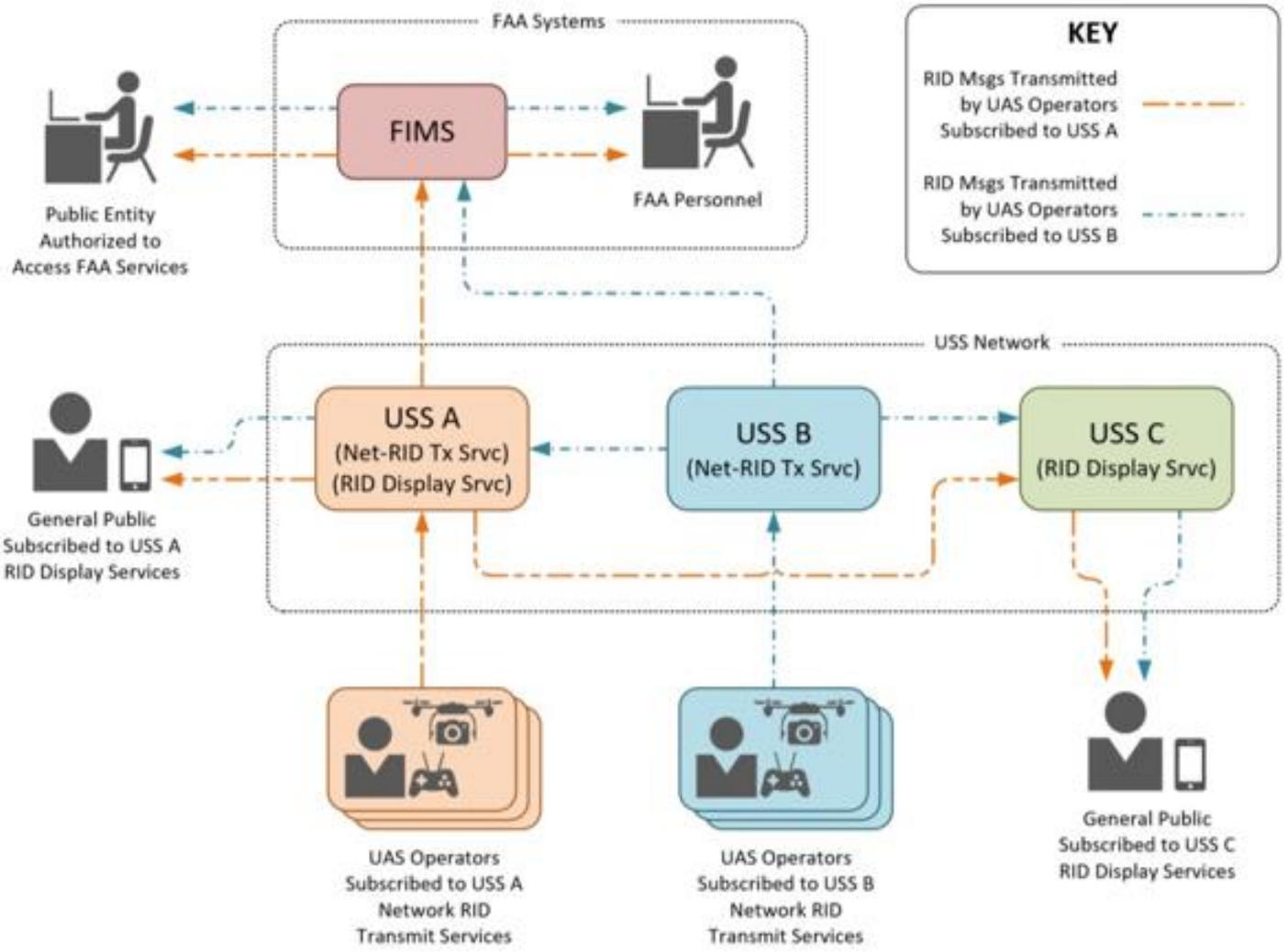


Figure 9-1: Remote ID Message Transmission via Network Publication Flow

UPP2 Use Case 5

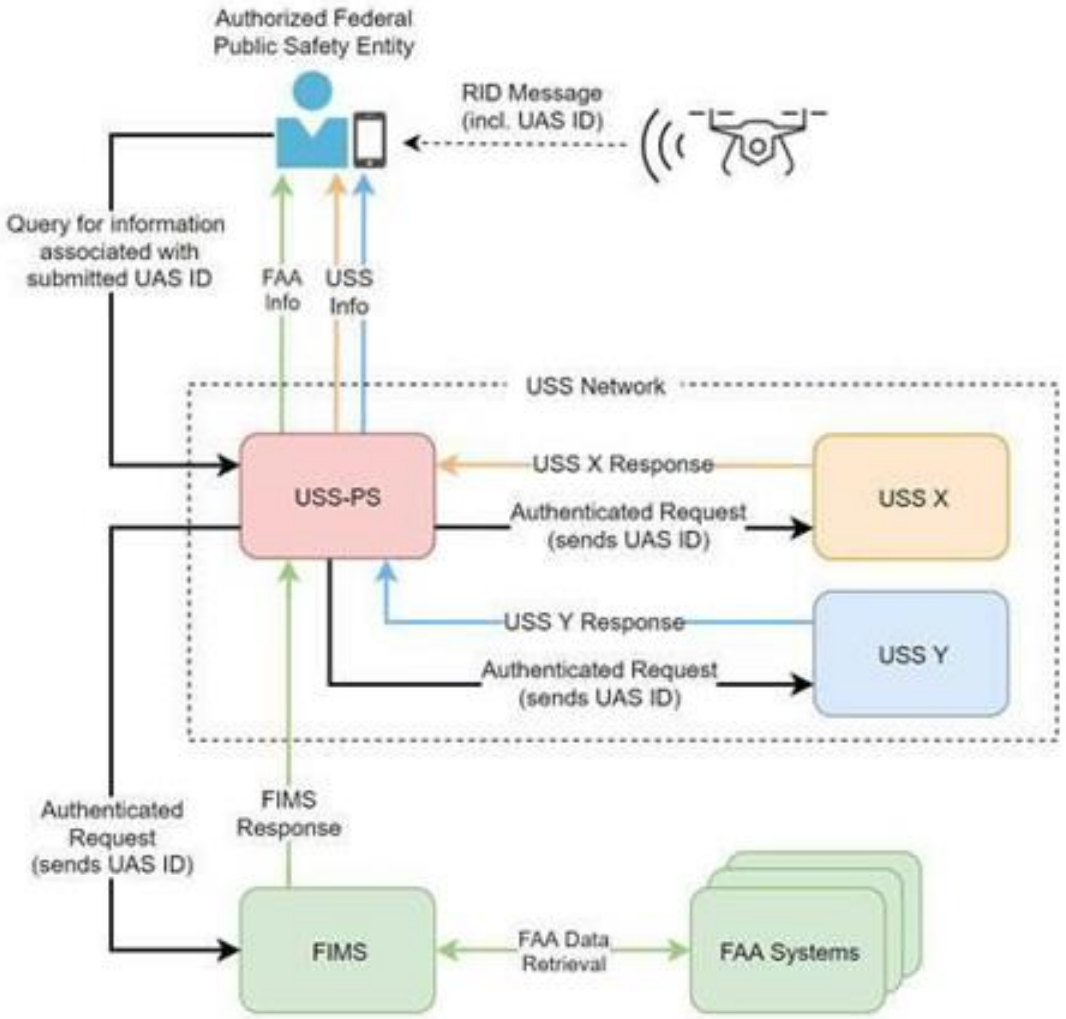


Figure 10-1: Direct Query to FAA and USS Network

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

- Focused on message formatting & performance
- 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 GCS -> cellular LTE -> Internet -> NETSP
  - 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
  - Only NETSP<->NETDP is fully specified, uses JSON / RestAPI
- Security methods punted to implementors, only framing specified

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 EU 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**

Gap analysis

- 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…

Requirements Methodology
(thanks to Andrei Gurtov for input)

- Current draft requirements driven by constraints imposed by
  - In-flux rule development by some but not all cognizant regulators
  - Design choices made by some but not all other SDOs working in the area
- Some of these may not apply in some specific contexts (see Andrei's tm-rid list post)

  e.g. if other comm channels (LDACS?) or nets (5GAA?) are supported
- How do we move forward w/necessary speed in light of the above?
  - 2-stage approach
    - Focus 1st on most urgent reqs, regulators, SDOs
    - Consider a –bis version after others chime in & things settle down
  - Attempt to address both currently written & suspected future reqs in 1 doc now
  - Any other suggestions?

Top Level DRIP Requirements & Approach

- UAS RID should be **immediately actionable**:
  - Trustworthy *information*
  - Show whether *operator* is trusted, even w/o observer Internet connectivity
  - Enable instant Observer to Pilot & M2M secure comms, when IP connectivity is available between endpoints

  Privacy must be maintained if not forfeited by the UAS operator through clueless, careless or criminal actions

- Complement existing external standards
  - ANSI, ASTM (F38.02 participation), CTA, EUROCAE/RTCA, ICAO (Trust Framework Study Group [TSFG] Trust Reciprocity Operational Needs [TRON] participation), CAAs…
  - FAA cites ASTM F3411-19 as potential means of compliance… but security & threat model not addressed!
- Leverage existing Internet business models, services, infrastructure, protocols & IETF expertise
  - Complement ASTM F3411-19 to mitigate a few shortfalls
  - Support a variety of applications related to UAS RID (e.g. V2X, DAA, C2)
- Stretch goal: integrate sources of track information other than operator self-reports
  - Gateway Broadcast RID to Network RID
  - Enable multilateration of relayed reports

Summary of Proposed DRIP Architecture (1 of 2):
Updated ASTM F3411 + Updated Selected IETF Standards

- Mapping an observed UA's **physical location -> UAS ID** similarity to the inverse problem of mapping an Internet **host ID -> logical location** (IP address) inspired leveraging IETF standard Host Identity Protocol (HIP), which then brought other benefits, so…
- We propose 2 minor tweaks to the ASTM F3411-19 UAS RID application standard.
  - Define a UAS ID Type (presumably 4) as a Hierarchical Host Identity Tag (HHIT).
  - Allow full 10 BT4 pages of Authentication Message to contain authentication data.
- We propose several updates/enhancements to the IETF HIP standards.
  - New crypto must be integrated to fit signatures & certificates in tiny Bluetooth packets.
  - Host Identity Tags (HITs) must be extended to allow for a registry Hierarchy (HHITs).

Summary of Proposed DRIP Architecture (2 of 2):
Updated ASTM F3411 + Updated Selected IETF Standards

- We propose using
  - EPP to populate UAS ID = Internet [pseudo-]domain name registries w/private & public data
  - RDAP w/access controls (e.g. XACML, OAuth) to query them for private data
  - DNS to hold minimal public data (standard RR types, plus maybe a typical TXT RR cheat)
- We have implemented ~baseline ASTM F3411-19 (we referenced OpenDroneID as a model, wrote our own Python code) & prototyped some of these proposed extensions.
  - We have flown successfully test flown some of this at the NY UAS Test Site.
  - We have updated our prototypes to authenticate UAS RID claims & will soon fly again.