Drone Remote Identification Protocol (DRIP)

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

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

interim meeting 2020 APR 22

draft-card-drip-**reqs-02** & -arch-02

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.

FAA's UTM Pilot Project 2 (UPP2) Architecture

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

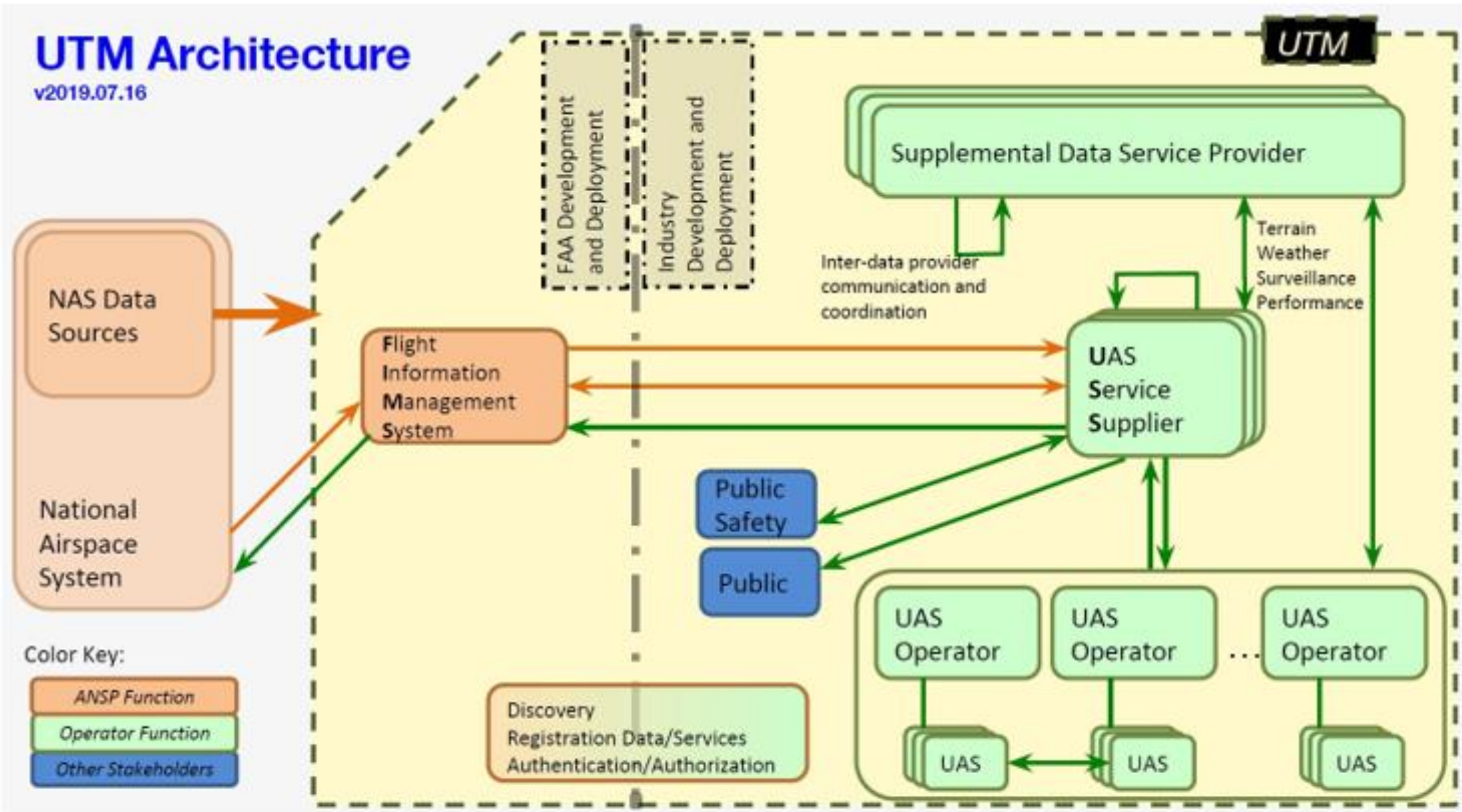


Figure 4-1: Notional Architecture

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

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

UPP2 Use Case 4

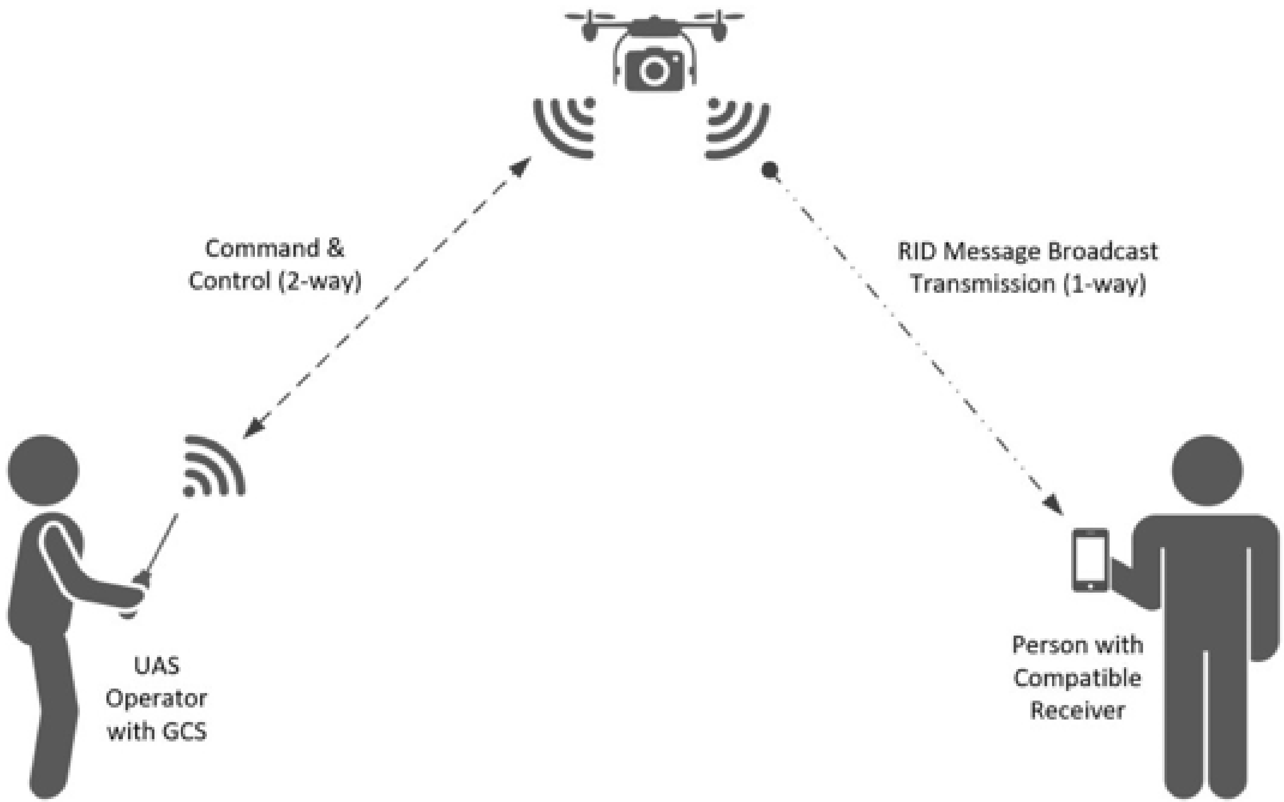


Figure 9-2: Remote ID Message Transmission via Broadcast

UPP2 Use Case 4

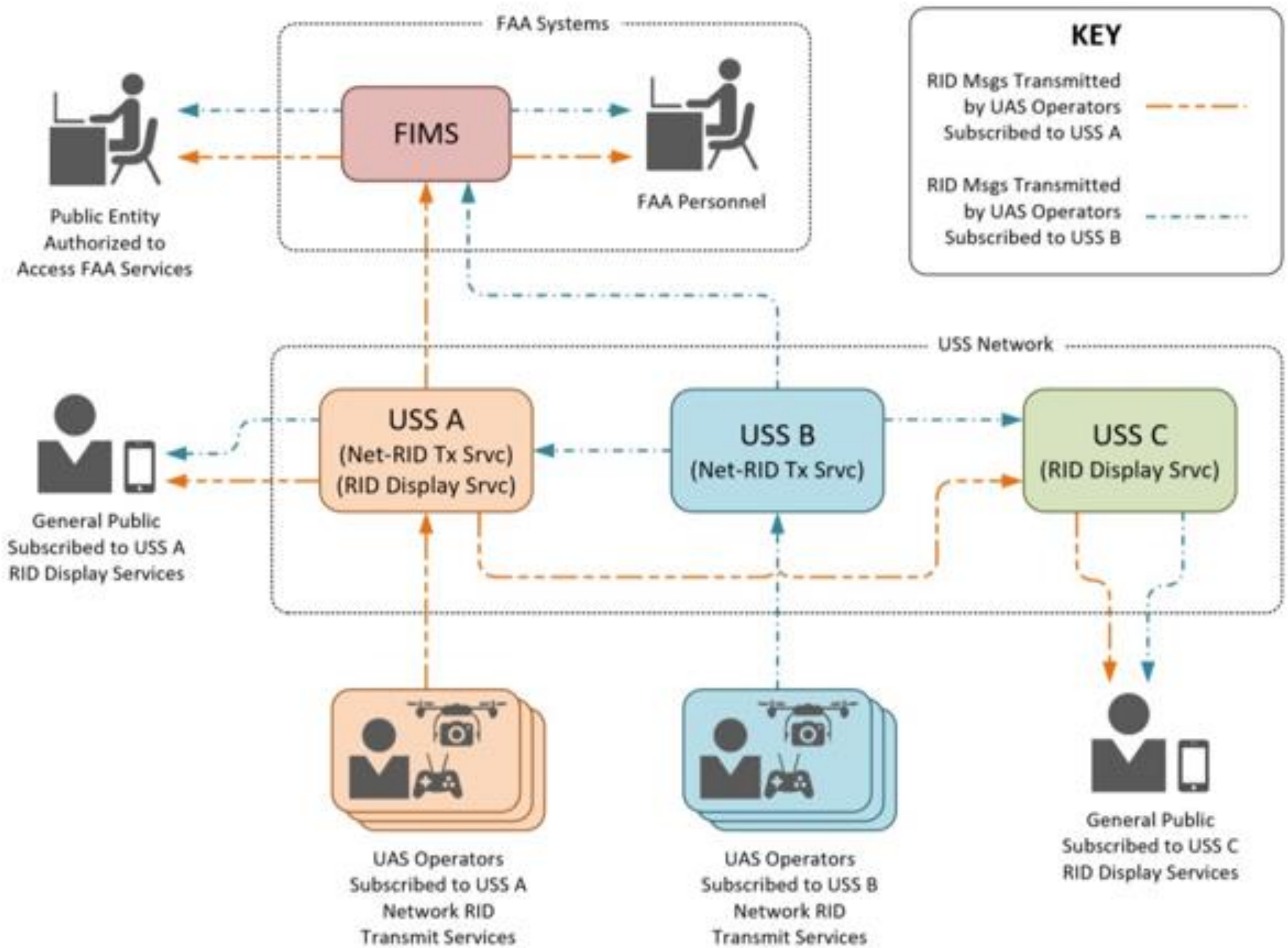


Figure 9-1: Remote ID Message Transmission via Network Publication Flow

Regulations & 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…

UPP2 Use Case 5

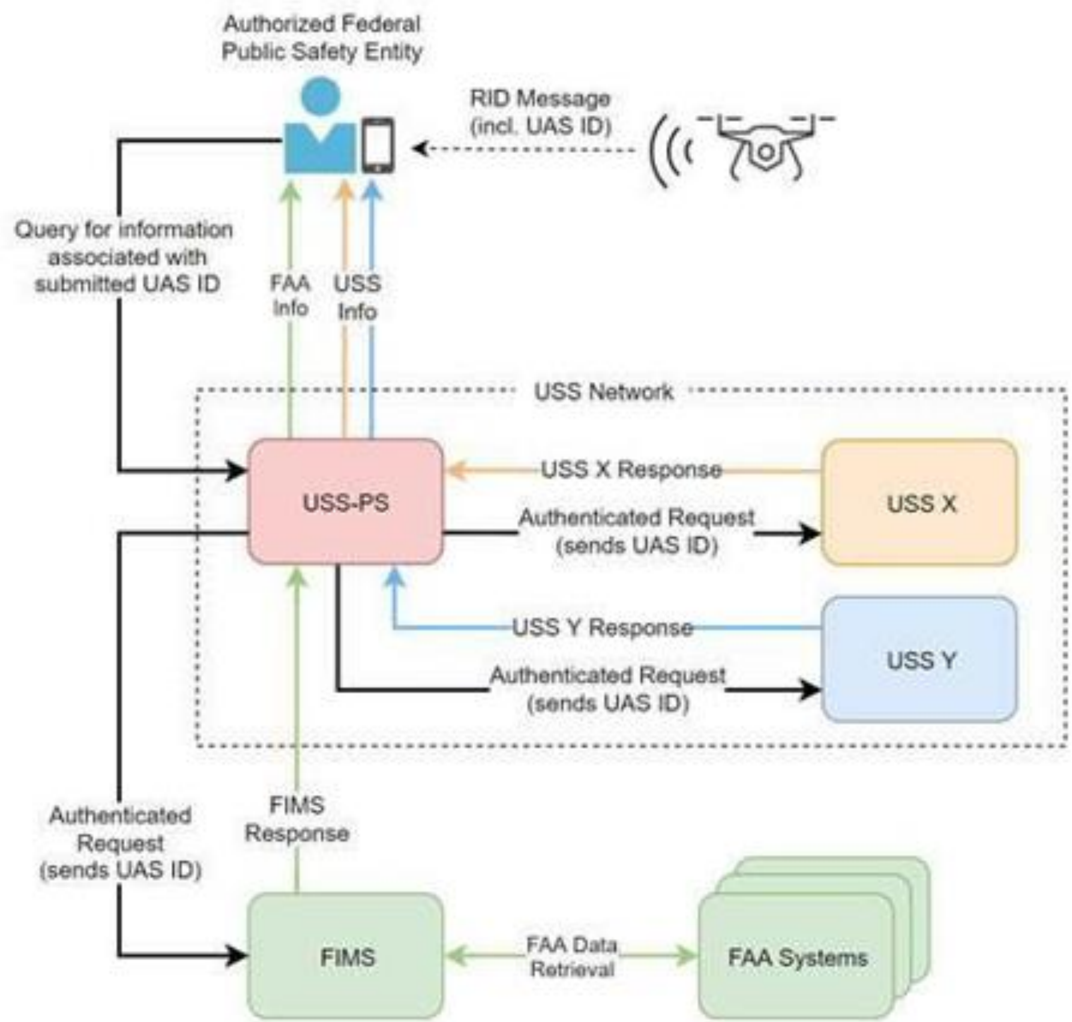


Figure 10-1: Direct Query to FAA and USS Network

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

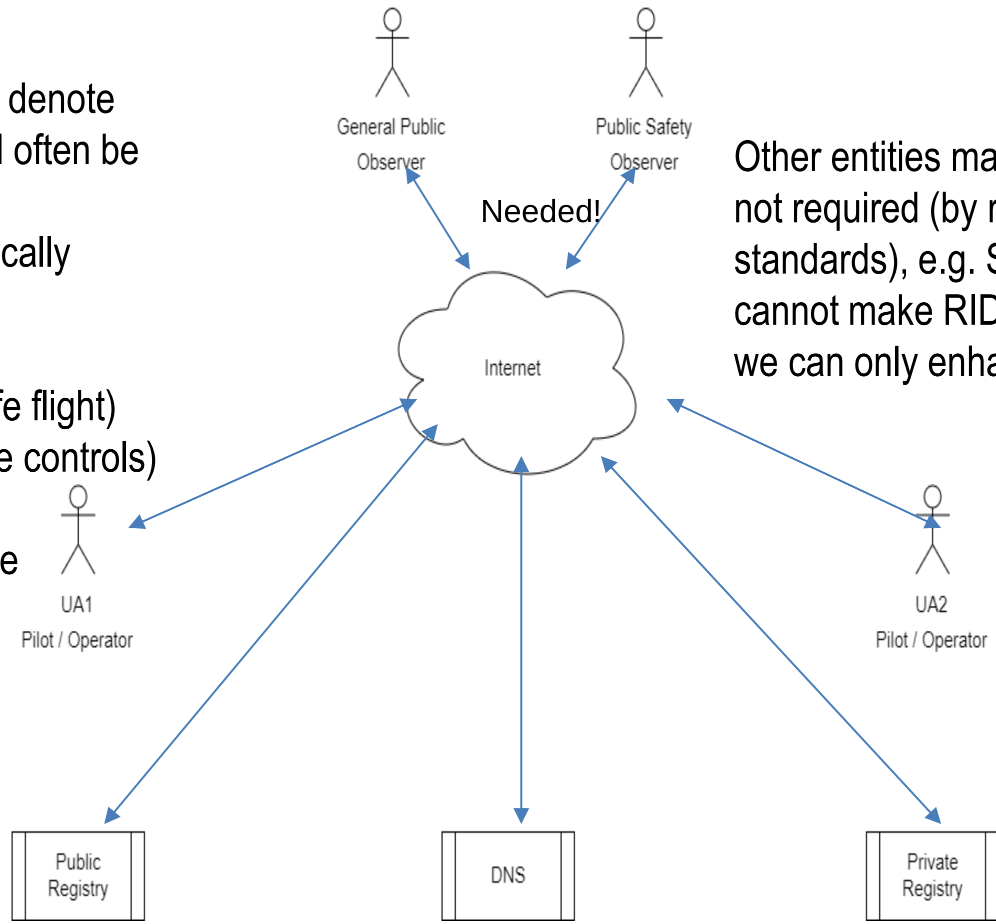
“Reference Architecture”:

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

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).

- **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 (with UAS ID Type 3, the same sender may have multiple IDs, potentially in different registries, but each ID should clearly indicate in which registry it can be found).

DRIP General Requirements

- **GEN-4 Public Lookup**

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

- **GEN-5 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).

- **GEN-6 Readability**

DRIP MUST enable information to be read and utilized by both humans and software.

- **GEN-7 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.

DRIP General Requirements

- **GEN-8 AAA Policy**

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

- **GEN-9 Finger (placeholder name)**

DRIP 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.

- **GEN-10 QoS**

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

DRIP General Requirements

- **GEN-11 Mobility**

DRIP MUST support physical and logical mobility of UA, GCS and Observers. DRIP SHOULD support mobility of all participating nodes.

- **GEN-12 Multihoming**

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

- **GEN-13 Multicast**

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

- **GEN-14 Management**

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

DRIP General Requirements

- It is highly desirable that Broadcast RID receivers be able to stamp messages with accurate date/time received and receiver location, then relay them to a network service (e.g. SDSP or distributed ledger). This supports 3 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
  - support optional SDSP services such as multilateration (to complement UAS position self-reports with independent measurements)

DRIP Identifier Requirements

- **ID-1 Length**

The DRIP [UAS] entity [remote] identifier must be no longer than 20 bytes.

- **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

- 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.
- 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.

- As satisfying these requirements may require that authorized actors have e.g. Internet connectivity 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 Requirements Conclusion (for now)

- Does requirements list
  - Have non-requirements that should be deleted?
  - Miss any requirements that should be added?
  - Contain overlaps or conflicts?
  - Need restructuring of classes?
  - Need point-by-point justification/rationale?
  - …?
- Next steps: gather any essential inputs from beyond ASTM, EASA, FAA

  ICAO IATF/GRAIN, EUROCAE/RTCA, IEEE, 3GPP?

➢ **Call for WG adoption of draft-card-drip-reqs-02 is open, ends MAY 04, please respond!**

Drone Remote Identification Protocol (DRIP)

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

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

interim meeting 2020 APR 22

draft-card-drip-reqs-02 & **-arch-02**

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

adam.wiethuechter@axenterprize.com

Robert Moskowitz rgm@labs.htt-consult.com

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

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.

DRIP Architecture Conclusion (for now)

- Although draft-card-drip-arch-02 definitely needs work, perhaps it is good enough to serve as a basis for *group* work, so does the WG wish to adopt it?
- Next steps for that draft: clarify what are
  - pre-existing UAS RID / UTM / U-space architecture into which DRIP must fit
  - essential DRIP architecture, independent of specific protocols
  - set of protocols that could implement that architecture
- Potential issues: harmonization among
  - Different US, EU, etc. regulations
  - ASTM F38.02 reluctance to revise F3411 until FAA (at least) issues final rules
  - Various other IETF efforts related to (mostly manned) aviation

Drone Remote Identification Protocol (DRIP)

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

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

interim meeting 2020 APR 22

draft-card-drip-reqs-02 & -arch-02

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

adam.wiethuechter@axenterprize.com

Robert Moskowitz rgm@labs.htt-consult.com

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)

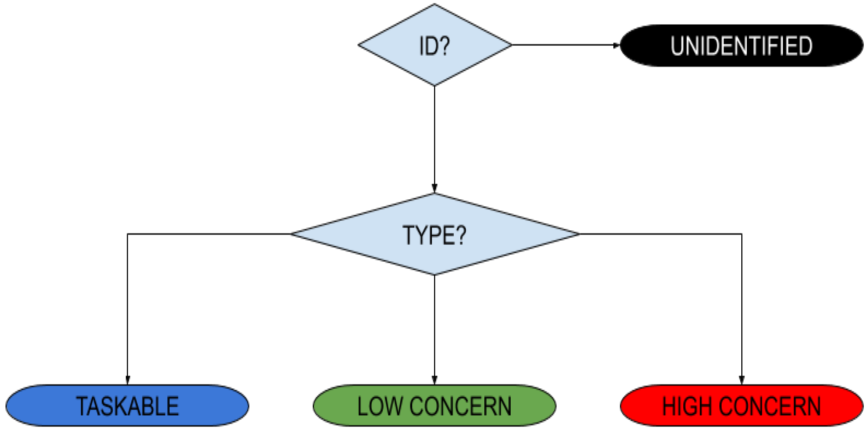
- **USS:** UAS Service Supplier
- SDSP: Supplemental Data Service Provider
- **UTM:** UAS Traffic Management (distributed system inc. many USS, SDSP, etc., hoped to scale better than humans using voice comms for Air Traffic Control [ATC])
- UVR: UAS Volume Reservation (temporary no-fly zone for most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

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.
  - FAA has declared that in the US, there will be no operations over people until UAS RID is deployed
- 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…
- Until UTM w/multiple interoperating USS is deployed, in US we have a partial solution:
  the Low Altitude Authorization & Notification Capability (LAANC)
- UTM is a moving target… but we still need to hit it…
  - 2 architectures still being debated – federated *vs* global
  - InterUSS Discovery & Synch. Service – most USS prototypes don't yet fully 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
  - ICAO International Aviation Trust Framework (IATF) / Global Resilient Aviation Interoperable Network (GRAIN)
- Urban/Advanced Air Mobility (UAM/AAM, think robotic air taxi) & EU U-Space (UTM/ATM) requirements – just beginning to be considered…

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)
- The sole fully ASTM F3411-19 specified Network RID interface is Net-RID SP <-> Net-RID DP but FAA NPRM does not recognize the latter as a distinct entity
- 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

Some network issues compounded by aero comms, constraining solutions

- Today's Internet has significant weaknesses in (esp. intersections of)
  - Mobility, Multicast, Multihoming
  - Management, QoS, Security
- Aero wireless networking compounds these
  - Each non-trivial aircraft has multiple radios of different types
  - Many types of radios hand off between base stations frequently
  - Most open standard protocols are challenged by
    - Low data rates, High error (or loss) rates, Long latencies
    - Link asymmetry, Rapid wide variation in channel characteristics
- ASTM F3411-19, per regulator guidance to support current smartphones as observer devices, imposes further constraints
  - One-way Bluetooth 4 advertisement (beacon) broadcast frames carry at most 24 bytes of payload
  - Paged multi-frame messages carry at most 224 bytes (minus any error control) to hold a signed message or certificate
- Security protocols requiring cryptographic processing are further challenged by
  - Limited on-board processing power
  - Brief contact time w/fast moving platforms
- Yet enormous safety implications (e.g. drone crashes into people or critical infrastructure) of insecure or unreliable protocols
- Aggregation of enough publicly broadcast RID transmissions enables inference of sensitive information about the physical world (e.g. air operations routes & schedules)

Context for Architectural Design

- An ID is not an end in itself

  It exists to enable
  - Public information lookups
  - Private information lookups w/AAA per policy
  - Dynamic establishment of secure comms between Observer & Pilot
  - Facilitation of related services: V2X, DAA, C2…
- UAS RID design considerations

  Urgent need for near-universal deployment, so support
  - Observers w/legacy smartphones -> Bluetooth 4 beacons, WiFi NaN (so far)
  - Non-equippable UA -> Net-RID from GCS (or operator phone)
  - Consumer toys & other small UA -> very low $SWaP
  - Internet-disconnected UA [& Observer devices]
- DRIP goals

  Leverage Internet standard protocols, services, infrastructure & business models to ensure
  - Trustworthy information: ID & other data provided via UAS RID
  - RID message privacy (PII protection)
  - Secure UA -> ground comms inc. Broadast RID
  - Broadcast RID “harvesting” & secure forwarding into UTM/U-space
  - Secure UAS -> Net-RID SP comms

DRIP drafts

- Basic DRIP for UAS RID
  - draft-card-drip-reqs-02: today's focus; adopt?
  - draft-card-drip-arch-02: next step; needs help
  - solution space
    - draft-wiethuechter-drip-auth-00: message formats
    - draft-wiethuechter-drip-identity-claims-00
    - draft-moskowitz-drip-operator-privacy-01
- DRIP extensions beyond UAS RID as contemplated by ASTM & regulators
  - draft-moskowitz-drip-crowd-sourced-rid-03
    - gateway Broadcast RID into Network RID for best of both
    - independent measurements & multilteration to confirm operator self-reported location
  - draft-moskowitz-drip-secure-nrid-c2-00
    - F3411: UAS shall authenticate w/Net-RID SPs using an industry-standard authentication mechanism; communication between UAS & Net-RID SPs shall be encrypted using an industry-standard encryption mechanism w/a minimum encryption strength of 128 bits
    - FAA NPRM: FAA Order 1370.121; InfoSec / Privacy Program & Policy; NIST standards; cybersecurity protections are necessary to defend against cyber threats that could adversely affect the authenticity or integrity of the remote identification information being transmitted by the UAS to a Remote ID USS or being broadcast from the UA

Related IETF Work

- drafts supporting DRIP & potential extensions by Bob *et al*
  - draft-moskowitz-hip-fast-mobility-03
  - *draft-moskowitz-hip-hhit-registries-02*
  - *draft-moskowitz-hip-hierarchical-hit-04*
  - *draft-moskowitz-hip-new-crypto-04*
  - *draft-moskowitz-orchid-cshake-00*
  - draft-moskowitz-ecdsa-pki-08
  - draft-moskowitz-eddsa-pki-03
  - draft-ietf-hip-dex-18
  - draft-ietf-hip-rfc4423-bis-20
- Other work to watch
  - draft-maeurer-raw-ldacs-02
  - draft-haindl-lisp-gb-atn-04
  - draft-templin-v6ops-icao-int-00
  - draft-templin-intarea-6706bis-45
  - draft-templin-atn-aero-interface-20
  - draft-ietf-rtgwg-atn-bgp-05

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
  - enable observers to instantly determine UAS operator trust class (even w/o Internet)
  - enable observers to instantly establish secure comms w/operator (w/IP connectivity)
  - enable observers to confirm observer-claimed location & velocity
- Aviators familiar w/radio comms, not networking; IETF can help
  - leverage existing Internet businesses/services/infrastructure/protocols
  - 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…**