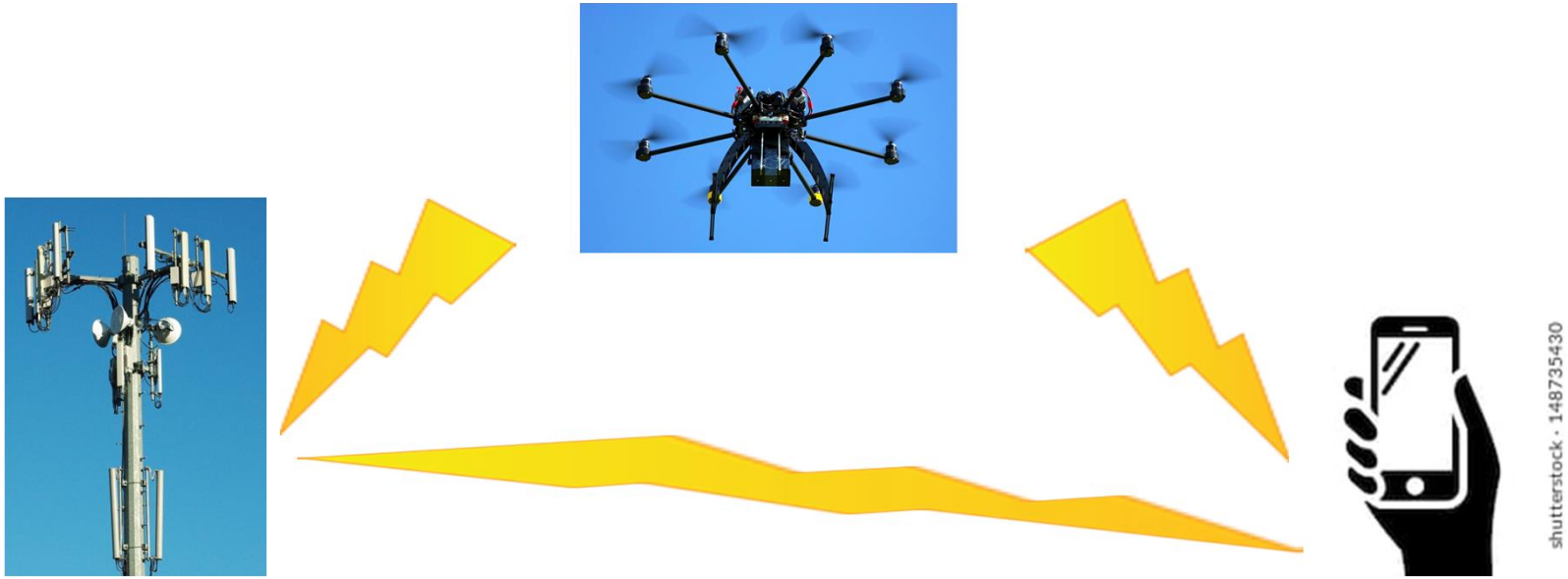

Drone Remote Identification Protocol (DRIP)

2020 AUG 26 update on

draft-ietf-drip-reqs

now at rev -04

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

Summary of Changes to -reqs
since IETF 108

what I did & didn't do as editor:

(0) did attempt to address every point raised by reviewers (to the extent I thought I understood them);

(1) didn't take suggestions apparently due to reviewer lacking UAS context, instead added missing context;

(2) didn't take suggestions apparently lacking consensus (but will if raised again & WG expresses consensus);

(3) didn't remove definitions of terms likely to be used in other DRIP documents (but will if the WG prefers);

(4) didn't substantially restructure the document (but will if the WG prefers);

(5) didn't do all the minor corrections & final proofreading (yet).

Michael R. review comment

Should GEN-1 be exploded into multiple numbered requirements?

(a) message integrity / non-repudiation

(b) defense against replay attacks

(c) defense against spoofing

(d) connected to a sender public key (related to GEN-3)

(e) Observer w/o Internet at time of observation

DRIP General Requirements

Å GEN-1 Provable Ownership (explode into multiple reqs per Michael R?)

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.

Å 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.

Å 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 replay attacks; and support optional SDSP services such as multilateration (to complement UAS position self-reports with independent measurements).

- **GEN-6 Finger**

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. (Daniel says we should try to define)

- **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).

- **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).

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 (revised per previous debate)**

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. DRIP MUST NOT encrypt safety critical data to be transmitted over Broadcast RID in any situation where it is unlikely that local observers authorized to access the plaintext will be able to decrypt it or obtain it from a service able to decrypt it. DRIP MUST NOT encrypt data when/where doing so would conflict with applicable regulations or CAA policies/procedures, i.e. DRIP MUST support configurable disabling of encryption.

- **PRIV-3 Encrypted Storage (previously revised per prior debate)**

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

DRIP Privacy Requirements

- **PRIV-4 Public/Private Designation (new)**

DRIP SHOULD facilitate designation, by cognizant authorities and information owners, which information is public and which private. By default, all information required to be transmitted via Broadcast RID, even when actually sent via Network RID, is assumed to be public; all other information contained in registries for lookup using the UAS ID is assumed to be private.

- **PRIV-5 Pseudonymous Rendezvous (new)**

DRIP MAY enable mutual discovery of and communications among participating UAS operators whose UA are in 4-D proximity, using the UAS ID without revealing pilot/operator identity or physical location.

- **Unnumbered explanatory text (expanded)**

How information is stored on end systems is out of scope for DRIP. Encouraging privacy best practices, including end system storage encryption, by facilitating it with protocol design reflecting such considerations, is in scope. Similar logic applies to methods for designating information as public or private.

The privacy requirements above are for DRIP, neither for [F3411-19] (which requires obfuscation of location to any Network RID subscriber engaging in wide area surveillance, limits data retention periods, etc. in the interests of privacy), nor for UAS RID in any specific jurisdiction (which may have its own regulatory requirements). The requirements above are also in a sense parameterized: who are the "authorized actors", how are they designated, how are they authenticated, etc.?

DRIP Registries Requirements

Å REG-1 Public Lookup

DRIP MUST enable lookup, from the UAS ID, of information designated by cognizant authority as public, and MUST NOT restrict access to this information based on identity of the party submitting the query.

Å REG-2 Private Lookup

DRIP MUST enable lookup 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), and MUST, per policy, enforce AAA, including restriction of access to this information based on identity of the party submitting the query.

Å 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.

Å 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.