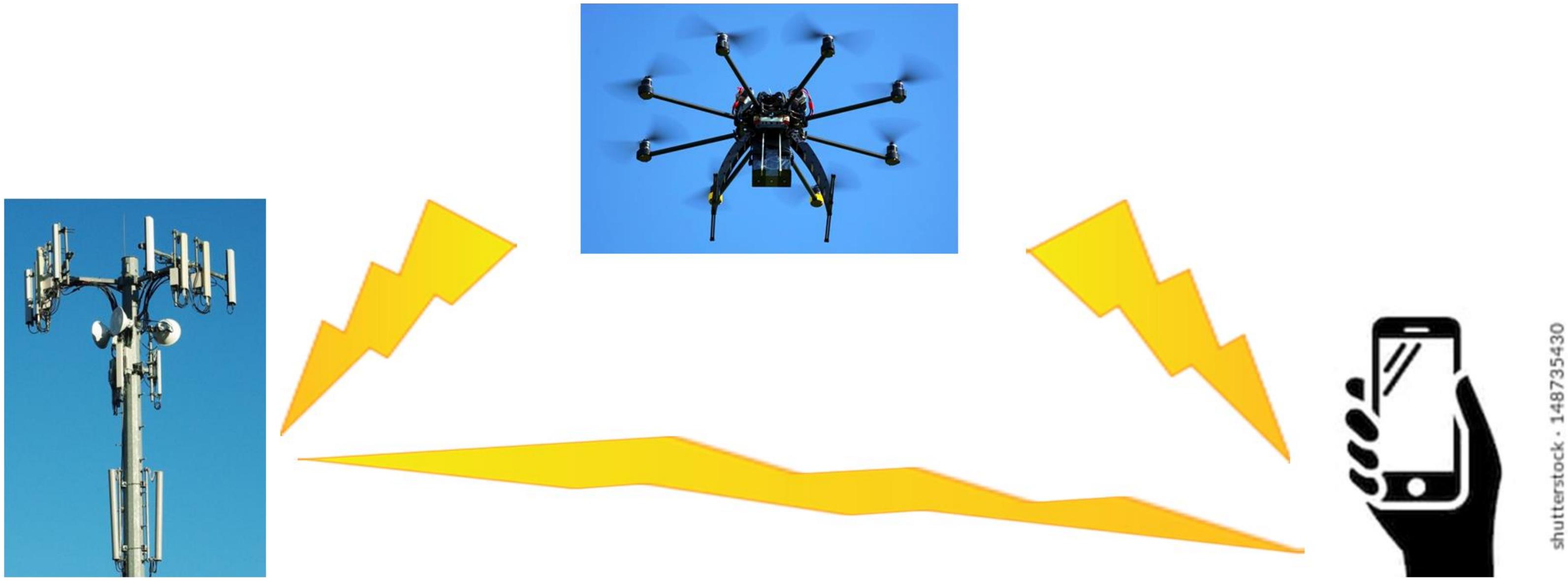

Drone Remote Identification Protocol (DRIP)

2020 SEP 23 update on
draft-ietf-drip-reqs
rev -05 in progress per prior consensus

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

Summary of Proposed Changes to -reqs

since August interim per apparent WG consensus

1) list Michael R's inferred sub-requirements of GEN-1 Provable Ownership but not make them separate numbered requirements

2) specify scope of ID-4 Uniqueness

3) minor restructuring & corrections per Amelia, Michael, Daniel, Med

NOTE: I have not yet processed comments received in the past 3 days, primarily the review from Fanny P., thank you!

ARCH: I have failed to update it as yet. A significant new contribution, in response to input from Alexandre P., is Stephan W's blurb on ADSB: the technical reasons why regulators are prohibiting its use for UAS RID.

DRIP General Requirements

Å **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.

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.

Security Considerations

proposed text to be added re: GEN-1 etc.

It may be inferred from the Section 4.1 General requirements for Provable Ownership, Provable Binding and Provable Registration, together with the Section 4.2 Identifier requirements, that DRIP must provide:

a) message integrity / non-repudiation

b) defense against replay attacks

c) defense against spoofing

One approach to so doing involves verifiably binding the DRIP identifier to a public key. Providing these security features, whether via this approach or another, is likely to be especially challenging for Observers without Internet connectivity at the time of observation. E.g. checking the signature of a registry on a public key certificate received via Broadcast RID in a remote area presumably would require that the registry's public key had been previously installed on the Observer's device, yet there may be many registries and the Observer's device may be storage constrained, and new registries may come on-line subsequent to installation of DRIP software on the Observer's device. Thus there may be caveats on the extent to which requirements can be satisfied in such cases, yet strenuous effort should be made to satisfy them, as such cases, e.g. firefighting in a national forest, are important.

DRIP Identifier Requirements

proposed text to be added specifying scope

Å **ID-4 Uniqueness**

The DRIP identifier MUST be unique within the global UAS RID identifier space from when it is first registered therein until it is explicitly de-registered therefrom.