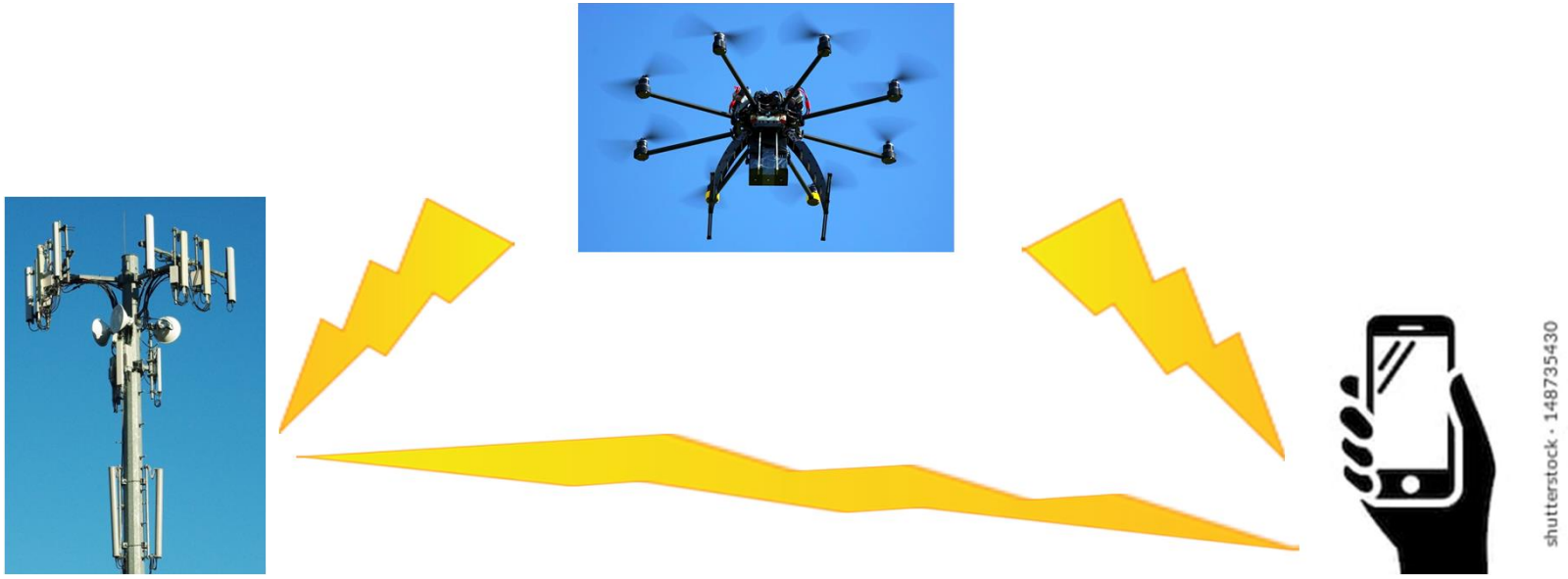


Drone Remote Identification Protocol (DRIP)

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

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

2020 JUL 30

draft-ietf-drip-reqs-03 & -arch-03

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.

News since JUN 24

- ASTM
  - ballot on Work Item WK59317 *Standard Specification for Vertiport Design*

    "Two-way radio communication for manned aircraft or equivalent level of control for unmanned aircraft, is maintained with the aircraft involved and pertinent traffic information is issued to all participating aircraft"
  - ballot on WK73458 / WK73459 revision to F3341 *Terminology for UAS*

    we should check our definitions, if ASTM & ICAO conflict, then what?
  - ballot on WK73701 re-approval of F2851 *Practice for UAS Registration and Marking (excluding Small UAS)*

    we should review
  - my review of *UTM Service Supplier (USS) Interoperability Standards v0.1* (WK63418? not marked)

    Monitoring USS must notify operator (?!) if RID position updates are not received reliably at required rates
- FAA
  - Jay Merkle, Exec. Director, UAS Integration "There are many areas in the US where network coverage is not available. For this reason the FAA included a broadcast mode of RID to augment network coverage."

    confirms broadcast RID authentication cannot depend upon Observers having Internet connectivity in the field
  - Drone Advisory Committee draft comments on *FAA UTM CONOPS v2.0*

    emphasizes need for more clarity & detail, inc. explicitly specifically Net-RID, suggests CS-RID but not by name
- IATF Aviation Trust Framework Study Group (IATF/TFSG)
  - prototype CA began issuing X.509 certs to UTM Pilot Program 2 participants (*et al*?)
  - use case for digital ID for *all* aircraft drafted in TRON WG for consideration by DI WG
- Various government agency limited distribution memos – surprise ;-)

  want to maximize their surveillance of (inc. via CS-RID but not by name), yet minimize surveillance by, others, as well as avoid information leaks & system vulnerabilities via network interfaces of UAS RID, UTM, etc.

AT&T Foundry: *10 Bold Projections On The Future of Drones*

1. Drones will enable dynamic communications networks

2. Swarming technology will allow drones to work together

3. Algorithms will fly drones

4. Analytics will be performed in real time, on board drones

5. Drones will never have to land

6. Drones will create a new category of immersive experiences

7. Drones will be an extension of ground vehicles or even become vehicles

8. Drones will carry out important tasks more safely than humans

9. Drones are the development platform of tomorrow

10. Secure IoT platforms will catalyze widespread adoption of drones

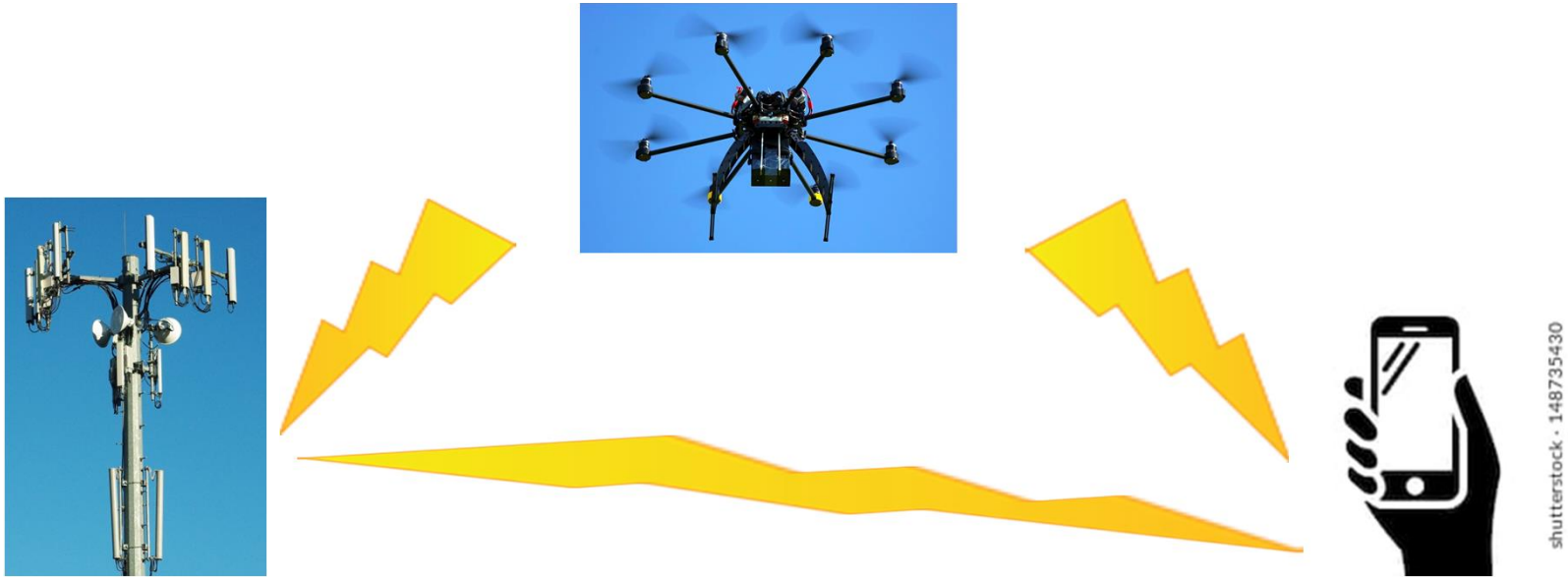
Status Reported JUN 24 & Related Topics

- Add more authors! Get more comments!
- Focus on registration
- Coordinate with IATF/TFSG
- Clarify definitions of UAS Operator *vs* Pilot in Command *vs* Remote Pilot
- Define Observer (possibly aboard a manned aircraft or [Operating] another UAS)
- Confirm definitions from user community standards esp. ICAO & ASTM
- Remove potential DRIP follow-on goals (beyond basic UAS RID) from -reqs?
- -reqs 5 Discussion/limitations: keep as is, make appendix or distribute content?
- -arch 7 EASA implications: keep as is, make appendix or distribute content?
- Expand CS-RID coverage? In –reqs or –arch?
- Organize set of related drafts
- Liaison w/RTCA & EUROCAE? Need help tracking them, EASA, EuroControl, IATA…
- Document use cases [not] justifying Observer to Pilot (O2P) comms

Summary of Activity since JUN 24

- Promising discussions w/domain registration experts (see Michael's slides)
- ICAO
  - IATF/TFSG (TRON, DI, GRAIN) semi-weekly intense liaison (thanks Bob, Fred & Sue!)

    DRIP-related HIP-based approach to ID for all aircraft [& aviation related ground nodes] receiving support
  - *UTM - A Common Framework with Core Principles for Global Harmonization* & *Doc 4444: ATM Procedures for Air Navigation Services* used as sources for definitions (thanks Saulo!)
- ASTM UAS RID chair productive back & forth clarification discussions
- ANSI Unmanned Aircraft Systems Standardization Collaborative (UASSC) published *Standardization Roadmap for Unmanned Aircraft Systems v2.0*
  - includes list of SDOs & UAS related activities, inc. many of which we were unaware, of note SAE AS-4UCS
  - now includes IETF esp. DRIP (thanks Bob!)
- Addressed most inputs received from AD, 2 WG co-chairs, 5 draft co-authors, 20 others
  - Jabber logs & minutes from 4 previous meetings all parsed
  - 100+ emails of inputs parsed (of 600+ DRIP-related received by me since May interim)
  - most but not yet all parsed inputs addressed in –reqs or –arch drafts (see following slides)



Drone Remote Identification Protocol (DRIP)

2020 JUL 30 update on

draft-ietf-drip-reqs

now at rev -03

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

Summary of Changes to -reqs
since IETF 107 & especially in -03

- Most minor content & editorial comments addressed
  - Thanks Eric, Daniel, Med, Amelia, Sue, Shuai, Ryan!
- Addition of explanatory prose
  - Mostly in areas where there was confusion in text, mostly missing UAS or more generally aviation context
  - “immediately actionable” explained at length
- Privacy & Transparency, see next 3 slides
- Open Issues, last slide in this section

Privacy & Transparency Considerations

- New section in -03
  - Motivated by many comments in BoF session during IETF 106
  - More comments in 1st DRIP meeting during IETF 107
  - Substantial input recently, thanks esp. Amelia!
- Per her check of -reqs *vs* RFC 6973, we weren't too bad
  - We are weak on 7.2 User Participation esp. Preference expression
  - "Defaults" was the only item found entirely missing from -02
  - Reviewers should check -03 *vs* RFC 6973 & RFC 8280!
- Supplements PRIV numbered requirements (see next 2 slides)
- Anything coming from pidloc side meeting in time for us?

PRIV-2 Encrypted Transport

- rev -03 numbered requirement (sorry, partly my solution-space thinking)

  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 unless also concurrently sending that data via Network RID and obtaining frequent confirmations of receipt.

- Bob's 1st suggestion (do we really want to drop E2E qualifier?)

  ... If transport is via IP, then encryption MUST be ~~end-to-end,~~ at or above the IP layer (not only beneath IP).

- Bob's 2nd suggestion (avoids solution-space ☺ but omits safety point ☹)

  ~~DRIP MUST NOT encrypt safety critical data to be transmitted over Broadcast RID unless also concurrently sending that data via Network RID and obtaining frequent confirmations of receipt.~~ Private data encryption MUST conform with CAA policies and procedures. That is there MAY be times and locations where encryption is NOT allowed and the UAS MUST be able to conform to these rules.

- ➢ After 2 more slides, please let's discuss

PRIV-3 Encrypted Storage

- rev -03 numbered requirement

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

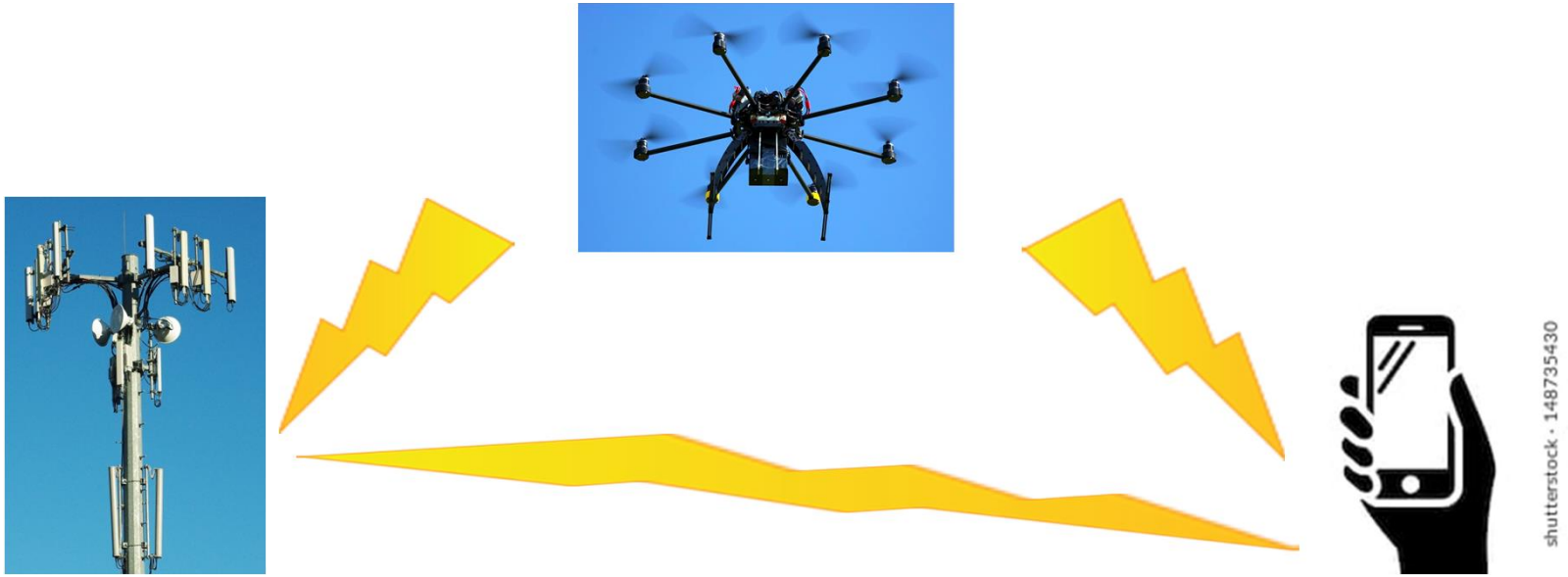
- rev -03 explanatory note

  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.

- Acceptable? Is it time for my first hum? ☺

Open Issues: take to tm-rid@ietf.org?

- Eric: cite regulator specific requirements? ~ Shuai: cite ASTM specific key performance indicators?
- Daniel
  - define authentication or other AAA components?
  - explicitly list & number constraints like requirements?
  - address how info should be linked and/or create a registry information model?
- Med (very thorough review, mostly addressed in -03 so only residuals listed below)
  - lots of minor editorial points
  - remove pointers to solution space docs
  - extract “Requirement could be met with” from definitions of “Direct Remote Identification” & “Network Identification Service” (move where)?
  - GEN-7 “QoS” -> “Performance” (but what about Reliability)?
  - GEN-11 Management: what is a “RID service”?
- Amelia (very helpful w/European perspective esp. on privacy)
  - cite EU / EuroControl Single European Sky ATM Research (SESAR) *Joint Undertaking Initial view on Principles for the U-space architecture* (need help knowing what points to cite where)?
  - reorganize Introduction into Uses, Privacy Concerns, Resource Constraints?
  - remove definitions of unused terms *vs* retain as glossary for other DRIP docs?
  - cross-tab DRIP numbered requirements *vs* RFC 6973 privacy checklist?
  - address RFC 6973 7.2 User Participation esp. control & preference expression
- Carsten: UAS [Pilot|Operator] <-> UAS [Pilot|Operator] use case?
- Ryan: replay attacks esp. “chaffing” the airspace volume?
- Stu: airspace volumes w/different RID rules?



Drone Remote Identification Protocol (DRIP)

2020 JUL 30 update on

draft-ietf-drip-arch

now at rev -03

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

Open Issues:
address few now, take rest to tm-rid@ietf.org

- Points not yet fully addressed [from reviews] on next 6 slides
  - Med
  - Bob
  - Amelia
  - list thread started w/Amelia's review
  - Daniel (review of -03)
  - Stu

Med's -02 review points as yet only partly addressed

- 1 Intro: ASTM NetRID/Broadcast-RID: shorten & augment w/pointers to -reqs 3.1 & 3.2
- 1 Intro: bullet list at end of section: replace w/text that introduces the -arch draft & its goals
- 1 or 3: provide picture of components & their interactions (before protocol-specific discussion)
- 3 Entities: Link to requirements
- 3.1.1.1 Background: is scalability driving hierarchy in –reqs?
- 3.2.2 Proposed Approach: what is a "standard" DNS server, e.g. do DoT/DoH qualify?

Bob's -02 review points as yet only partly addressed

- Several minor editorial points
- 3.1.2: "locatable" -> "findable" per RFC 7484
- Appendix A: "flight status" -> "operation status"?
- Ask ASTM UAS RID chair whether F3411-19 mandates, for Network RID, not only the data dictionary, but also the specific message formats used for Broadcast RID?
- 4.1 *et seq* X.509 interoperability: HHIT altSubjectName Certificate Signing Request as part of registration?
- 5, *inter alia*, summarizes processes in draft-wiethuechter-drip-auth & draft-wiethuechter-drip-identity-claims: keep, delete & cite, merge?
- 5: leaves registration details (esp. manufacturer serial number based HHITs) incompletely specified

Amelia's -02 review points as yet not addressed

- Safety (e.g. EUROCAE e-ID) *vs* Security (e.g. EASA Direct RID)?
- Accessibility, Internationalization, Localization, Outcome Transparency, CIA (RFC 8280, esp. WRT –arch 3.1.2 & DNS)?
- Privacy (RFC 6973 esp. WRT mapping –arch 3.1 & 3/2 to –reqs 4.4)?
- Does control of airspace ID imply control of corresponding airspace?
- Have we oversimplified architectural implications of requirements (4, 7)?
- Network-RID illustrated, Broadcast RID not, why?
- Material from –reqs on ASTM is redundant here.
- Speculation on activities of other SDOs is irrelevant here.
- Persistence of identifiers & linkage of Operator registration # w/manufacturer assigned UA serial #?
- Federation, Modularity & Privacy goals apply at what levels of U-space?
- Data minimization is not addressed.
- Some material here (mostly in 6) belongs in –reqs.

Subsequent thread points as yet not addressed

- Carsten: refinement of safety *vs* security distinction
- Alexandre
  - Are Urban Air Mobility (UAM) “air taxis” considered “unmanned” as pilot is remote?
  - IEEE is starting work to maintain continuity across MAC address randomization.
  - Might UAM use IEEE 802.11-OCB mode (formerly 802.11p) links at 5.9GHz?
  - What about ADS-B or other lower radio frequency links?
  - Multiple domain names on the same aircraft? Confused w/formation flying?
  - Correspondence of airframe painted & digital identifiers?
  - Is automotive Vehicle Identification Number (VIN) *vs* license plate number a parallel?
- Bob
  - Remotely piloted UAM aircraft are currently considered UAS.
  - 5G/LTE or IEEE 802.15.16t seem more likely than 802.11-OCB.
  - Simple assertions of IDs are unverifiable thus trivially spoofable.
  - UAM/UAS do not seem to be adopting automotive V2X but some IETFers seem to be.
  - How does an UA not built by a manufacturer get an ANSI/CTI-2063A serial number?
- Saulo: UAM aircraft are envisioned as autonomous

Daniel's -03 review points as yet not addressed

- WRT scope
  - Architectural implications of EASA requirements belong in –reqs.
  - Introductory material from –reqs is redundant here.
  - Document should be self-contained.
- WRT RID entities & data flows, clarify:
  - Network RID "client" is [browser] app on Observer's device
  - [Internet] connectivity requirements among UA, GCS, SP, DP…
  - what Broadcast RID can do w/ & w/o Observer Internet connectivity
  - that Broadcast RID transmits public info (obviating some registry lookups)
  - how Network RID is "less constrained" than Broadcast RID
  - what is meant by "method" & "hybrid
  - add Broadcast RID figure, show UA & GCS in that & Network RID figure
- WRT registries, clarify:
  - what information is static, what information is dynamic
  - who is supposed to be able to access which information
  - when registries are accessed in what RID operations
  - what are differences & relationships among public & private registries, DP, SP, USS
- WRT identifiers
  - why should RID be in reverse DNS lookup?
  - "the only way for any other UA to assert this RID would be to steal something from within the UA" is a strong claim, ignores possibility of identifier collisions.
  - call X.509 PKI not "standard" but "classical", describe it to justify why it won't work here
  - explain continuing role of some kind of CA even w/o X.509 PKI
  - expand on different uses of & relationship between optional manufacturer-assigned HI & subsequent single-use HIs
- This is a solution specific, not generic, architecture; which do we want?
  - uses MUST/SHOULD terminology
  - specifies HIP technology based architecture; if that is to be so, explain more fully the operation & role here of HIP
  - gives too many details on DNS RR types etc.

Stu's own questions/concerns

- RFC 7033 WebFinger to identify humans (e.g. Pilot)?
- [HIP RVS] proxy to enforce AAA policy on O2P flow initiation?
- draft scopes
  - **Caveat:** much of my frustration presumably derives from my own inadequate give & take on the mailing list.
  - I originally started to draft an Applicability Statement for UAS RID but was told to split it into -reqs & -arch.
  - The architecture into which DRIP must fit is defined by regulators & other SDOs: any architecture we define is either a redundant document or a specific solution approach; -reqs should drive -arch not vice-versa.
  - Reviews ask for both less & more context; much -arch confusion comes from reader lacking -reqs context.
  - Now Bob has drafted ~ an Applicability Statement for UAS RID.
  - Should we merge these 3 drafts?
- malicious Operator could register harmless toy, then provision weaponized UAS w/its private key!

  need CS-RID++ to share sensor data, e.g. video that could confirm/refute claimed UA type?