Workgroup: DRIP
Internet-Draft: draft-ietf-drip-reqs-00
Published: 18 May 2020
Intended Status: Informational
Expires: 19 November 2020
Authors: S. Card, Ed. A. Wiethuechter R. Moskowitz
AX Enterprize AX Enterprize HTT Consulting

Drone Remote Identification Protocol (DRIP) Requirements

Abstract

This document defines the requirements for Drone Remote Identification Protocol (DRIP) Working Group protocols and services to support Unmanned Aircraft System Remote Identification (UAS RID).

Objectives include: complementing external technical standards as regulator-accepted means of compliance with UAS RID regulations; facilitating use of existing Internet resources to support UAS RID and to enable enhanced related services; and enabling verification that UAS RID information is trustworthy (to some extent, even in the absence of Internet connectivity at the receiving node).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 November 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with

respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Many safety and other considerations dictate that UAS be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The United

States (US) Federal Aviation Administration (FAA) has published a Notice of Proposed Rule Making ([NPRM]). CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed ASTM F3411-19 [F3411-19] Standard Specification for Remote ID and Tracking. It defines 2 means of UAS RID. Network RID defines a set of information for UAS to make available globally indirectly via the Internet. Broadcast RID defines a set of messages for Unmanned Aircraft (UA) to transmit locally directly one-way over Bluetooth or Wi-Fi. Network RID depends upon Internet connectivity, in several segments, from the UAS to the observer. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the directly locally received UAS ID as a key. It is expected that the same information will be provided via Broadcast and Network RID; in the US, the FAA NPRM so specifies.

[F3411-19] specifies 3 UAS ID types. Type 1 is a static, manufacturer assigned, hardware serial number per ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A]. Type 2 is a CAA assigned (presumably static) ID. Type 3 is a UAS Traffic Management (UTM) system assigned UUID [RFC4122], which can but need not be dynamic. The EU allows only Type 1; the US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once (for a single UAS flight, which in the context of UTM is called an "operation"). [F3411-19] Broadcast RID transmits all information in the clear as plaintext (ASCII or binary), so static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g. package delivery routes of competitors.

An ID is not an end in itself; it exists to enable lookups and provision of services complementing mere identification.

Minimal specified information must be made available to the public; access to other data, e.g. UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized per policy. The balance between privacy and transparency remains a subject for public debate and regulatory action; DRIP can only offer tools to expand the achievable trade space and enable trade-offs within that space. [F3411-19] specifies only how to get the UAS ID to the observer; how the observer can perform these lookups, and how the registries first can be populated with information, is unspecified.

Using UAS RID to facilitate vehicular (V2X) communications and applications such as Detect And Avoid (DAA, which would impose tighter latency bounds than RID itself) is an obvious possibility, explicitly contemplated in the FAA NPRM. However, applications of RID beyond RID itself have been omitted from [F3411-19]; DAA has been explicitly declared out of scope in ASTM working group discussions, based on a distinction between RID as a security standard vs DAA as a safety application. Although dynamic establishment of secure communications between the observer and the UAS pilot seems to have been contemplated by the FAA UAS ID and Tracking Aviation Rulemaking Committee (ARC) in their [Recommendations], it is not addressed in any of the subsequent proposed regulations or technical specifications.

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by observers of already ubiquitous mobile devices (smartphones and tablets). Anticipating likely CAA requirements to support legacy devices, especially in light of [Recommendations], [F3411-19] specifies that any UAS sending Broadcast RID over Bluetooth must do so over Bluetooth 4, regardless of whether it also does so over newer versions; as UAS sender devices and observer receiver devices are unpaired, this implies extremely short "advertisement" (beacon) frames.

UA onboard RID devices are severely constrained in Size, Weight and Power (SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and observer receive RID capabilities. To accommodate the most severely constrained cases, all these conspire to motivate system design decisions, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges.

Given not only packet payload length and bandwidth, but also processing and storage within the SWaP constraints of very small (e.g. consumer toy) UA, heavyweight cryptographic security protocols are infeasible, yet trustworthiness of UAS RID information is essential. Under [F3411-19], even the most basic datum, the UAS ID string (typically number) itself can be merely an unsubstantiated claim. Observer devices being ubiquitous, thus popular targets for malware or other compromise, cannot be generally trusted (although the user of each device is compelled to trust that device, to some extent); a "fair witness" functionality (inspired by [Stranger]) may be desirable.

DRIP's goal is to make RID immediately actionable, in both Internet and local-only connected scenarios (especially emergencies), in severely constrained UAS environments, balancing legitimate (e.g. public safety) authorities' Need To Know trustworthy information with UAS operators' privacy. DRIP (originally called Trustworthy Multipurpose Remote Identification, TM-RID) potentially could be applied to verifiably identify other types of registered things reported to be in specified physical locations, but the urgent motivation and clear initial focus is UAS. Existing Internet resources (protocol standards, services, infrastructure, and business models) should be leveraged. A natural Internet architecture for UAS RID conforming to proposed regulations and external technical standards will be described in a companion DRIP Architecture document; this document describes only requirements.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Definitions

$SWaP
: Cost, Size, Weight and Power.

AAA
: Attestation, Authentication, Authorization, Access Control, Accounting, Attribution, Audit.

ABDAA
: AirBorne DAA. Also known as "self-separation".

AGL
: Above Ground Level. Relative altitude, above the variously defined local ground level, typically of an UA, typically measured in feet.

ATC
: Air Traffic Control. Explicit flight direction to pilots from ground controllers. Contrast with ATM.

ATM
: Air Traffic Management. All systems that assist aircraft from departure to landing. A broader functional and geographic scope and/or a higher layer of abstraction than ATC.

Authentication Message
: F3411 Message Type 2. Provides framing for authentication data, only.

Basic ID Message
: F3411 Message Type 0. Provides UA Type, UAS ID Type and UAS ID, only.

CAA
: Civil Aviation Authority. An example is the Federal Aviation Administration (FAA) in the United States of America.

C2
: Command and Control. A set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions. Mainly used in military contexts. In the UAS context, typically refers to the link between GCS and UA over which the former controls the latter. Out of scope for DRIP, even when this link is used to provide UA location to the GCS or vice-versa, for subsequent RID transmission.

DAA
: Detect And Avoid, formerly Sense And Avoid (SAA). A means of keeping aircraft "well clear" of each other for safety.

Direct RID
: Direct Remote Identification. Per [Delegated], "a system that ensures the local broadcast of information about a UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA". Requirement could be met with ASTM Broadcast RID: Basic ID message with UAS ID Type 1; Location/Vector message; Operator ID message; System Message. Corresponds roughly to the Broadcast RID portion of FAA NPRM Standard RID.

E2E
: End to End.

GBDAA
: Ground Based DAA.

GCS
: Ground Control Station. The part of the UAS that the remote pilot uses to exercise C2 over the UA, whether by remotely exercising

UA flight controls to fly the UA, by setting GPS waypoints, or otherwise directing its flight.

GPS
Global Positioning System. In this context, misused in place of Global Navigation Satellite System (GNSS) or more generally SATNAV to refer generically to satellite based timing and/or positioning.

GRAIN
Global Resilient Aviation Information Network. An effort to develop an international IPv6 overlay network with end-to-end security supporting all aspects of aviation.

IATF
International Aviation Trust Framework. ICAO effort to develop a resilient and secure by design framework for networking in support of all aspects of aviation.

ICAO
International Civil Aviation Organization. A United Nations specialized agency that develops and harmonizes international standards relating to aviation.

LAANC
Low Altitude Authorization and Notification Capability. Supports ATC authorization requirements for UAS operations: remote pilots can apply to receive a near real-time authorization for operations under 400 feet in controlled airspace near airports. US partial stopgap until UTM comes.

Limited RID
Per the FAA NPRM, a mode of operation that must use Network RID, must not use Broadcast RID, and must provide pilot/GCS location only (not UA location). This mode is only allowed for UA that neither require (due to e.g. size) nor are equipped for Standard RID, operated within V-LOS and within 400 feet of the pilot, below 400 feet AGL, etc.

Location/Vector Message
F3411 Message Type 1. Provides UA location, altitude, heading and speed, only.

LOS
Line Of Sight. An adjectival phrase describing any information transfer that travels in a nearly straight line (e.g. electromagnetic energy, whether in the visual light, RF or other frequency range) and is subject to blockage. A term to be avoided due to ambiguity, in this context, between RF-LOS and V-LOS.

MSL
: Mean Sea Level. Relative altitude, above the variously defined mean sea level, typically of an UA (but in FAA NPRM for a GCS), typically measured in feet.

Net-RID DP
: Network RID Display Provider. Logical entity that aggregates data from Net-RID SPs as needed in response to user queries regarding UAS operating within specified airspace volumes, to enable display by a user application on a user device. Under the FAA NPRM, not recognized as a distinct entity, but a service provided by USS, including Public Safety USS that may exist primarily for this purpose rather than to manage any subscribed UAS.

Net-RID SP
: Network RID Service Provider. Logical entity that participates in Network RID and provides to NetRID-DPs information on UAS it manages. Under the FAA NPRM, the USS to which the UAS is subscribed ("Remote ID USS").

Network Identification Service
: EU regulatory requirement for Network RID. Requirement could be met with ASTM Network RID: Basic ID message with UAS ID Type 1; Location/Vector message; Operator ID message; System Message. Corresponds roughly to the Network RID portion of FAA NPRM Standard RID.

Observer
: Referred to in other UAS RID documents as a "user", but there are also other classes of UAS RID users, so we prefer "observer" to denote an individual who has observed an UA and wishes to know something about it, starting with its ID.

Operator ID Message
: F3411 Message Type 5. Provides CAA issued Operator ID, only.

PII
: Personally Identifiable Information. In this context, typically of the UAS operator, Pilot In Command (PIC) or remote pilot, but possibly of an observer or other party.

RF
: Radio Frequency. May be used as an adjective or as a noun; in the latter case, typically means Radio Frequency energy.

RF-LOS
: RF LOS. Typically used in describing operation of a direct radio link between a GCS and the UA under its control, potentially subject to blockage by foliage, structures, terrain or other vehicles, but less so than V-LOS.

Self-ID Message
: F3411 Message Type 3. Provides a 1 byte descriptor and 23 byte ASCII free text field, only.

Standard RID
: Per the FAA NPRM, a mode of operation that must use both Network RID (if Internet connectivity is available at the time in the operating area) and Broadcast RID (always and everywhere), and must provide both pilot/GCS location and UA location. This mode is required for UAS that exceed the allowed envelope (e.g. size, range) of Limited RID and for all UAS equipped for Standard RID (even if operated within parameters that would otherwise permit Limited RID). The Broadcast RID portion corresponds roughly to EU Direct RID; the Network RID portion corresponds roughly to EU Network Identification Service.

SDSP
: Supplemental Data Service Provider. An entity that participates in the UTM system, but provides services beyond those specified as basic UTM system functions.

System Message
: F3411 Message Type 4. Provides general UAS information, including remote pilot location, multiple UA group operational area, etc.

U-space
: EU concept and emerging framework for integration of UAS into all classes of airspace, specifically including high density urban areas, sharing airspace with manned aircraft.

UA
: Unmanned Aircraft. An aircraft which is intended to operate with no pilot on board. In popular parlance, "drone".

UAS
: Unmanned Aircraft System. Composed of UA, all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and C2 links between UA and control station.

UAS ID
: UAS identifier. Although called "UAS ID", unique to the UA: neither to the operator (as previous registration numbers have been assigned), nor to the combination of GCS and UA that comprise the UAS. Per [F3411-19], maximum length of 20 bytes.

UAS ID Type
: Identifier type index. Per [F3411-19], 4 bits, values 0-3 already specified.

UAS RID
: UAS Remote Identification. System for identifying UA during flight by other parties.

UAS RID Verification Service
: System component designed to handle the authentication requirements of RID by offloading verification to a web hosted service.

USS
: UAS Service Supplier. Provide UTM services to support the UAS community, to connect Operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants. (From FAA UTM ConOps V1, May 2018).

UTM
: UAS Traffic Management. Per ICAO, "A specific aspect of air traffic management which manages UAS operations safely, economically and efficiently through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions." In the US, per FAA, a "traffic management" ecosystem for "uncontrolled" low altitude UAS operations, separate from, but complementary to, the FAA's ATC system for "controlled" operations of manned aircraft.

V-LOS
: Visual LOS. Typically used in describing operation of an UA by a "remote" pilot who can clearly directly (without video cameras or any other aids other than glasses or under some rules binoculars) see the UA and its immediate flight environment. Potentially subject to blockage by foliage, structures, terrain or other vehicles, more so than RF-LOS.

3. UAS RID Problem Space

UA may be fixed wing Short Take-Off and Landing (STOL), rotary wing (e.g. helicopter) Vertical Take-Off and Landing (VTOL), or hybrid. They may be single engine or multi engine. The most common today are multicopters: rotary wing, multi engine. The explosion in UAS was enabled by hobbyist development, for multicopters, of advanced flight stability algorithms, enabling even inexperienced pilots to take off, fly to a location of interest, hover, and return to the take-off location or land at a distance. UAS can be remotely piloted by a human (e.g. with a joystick) or programmed to proceed from Global Positioning System (GPS) waypoint to waypoint in a weak form of autonomy; stronger autonomy is coming. UA are "low observable": they typically have a small radar cross section; they make noise quite noticeable at short range but difficult to detect at distances

they can quickly close (500 meters in under 17 seconds at 60 knots); they typically fly at low altitudes (for the small UAS to which RID applies in the US, under 400 feet AGL); they are highly maneuverable so can fly under trees and between buildings.

UA can carry payloads including sensors, cyber and kinetic weapons, or can be used themselves as weapons by flying them into targets. They can be flown by clueless, careless or criminal operators. Thus the most basic function of UAS RID is "Identification Friend or Foe" (IFF) to mitigate the significant threat they present. Numerous other applications can be enabled or facilitated by RID: consider the importance of identifiers in many Internet protocols and services.

Network RID from the UA itself (rather than from its GCS) and Broadcast RID require one or more wireless data links from the UA, but such communications are challenging due to $SWaP constraints and low altitude flight amidst structures and foliage over terrain. Disambiguation of multiple UA flying in close proximity may be very challenging, even if each is reporting its identity, position and velocity as accurately as it can.

3.1. Network RID

Network RID has several variants. The UA may have persistent onboard Internet connectivity, in which case it can consistently source RID information directly over the Internet. The UA may have intermittent onboard Internet connectivity, in which case the GCS must source RID information whenever the UA itself is offline. The UA may not have Internet connectivity of its own, but have instead some other form of communications to another node that can relay RID information to the Internet; this would typically be the GCS (which to perform its function must know where the UA is). The UA may have no means of sourcing RID information, in which case the GCS must source it; this is typical under FAA NPRM Limited RID proposed rules, which require providing the location of the GCS (not that of the UA). In the extreme case, this could be the pilot using a web browser to designate, to an UAS Service Supplier (USS) or other UTM entity, a time-bounded airspace volume in which an operation will be conducted; this may impede disambiguation of ID if multiple UAS operate in the same or overlapping spatio-temporal volumes.

In most cases in the near term, if the RID information is fed to the Internet directly by the UA or GCS, the first hop data links will be cellular Long Term Evolution (LTE) or WiFi, but provided the data link can support at least IP and ideally TCP, its type is generally immaterial to the higher layer protocols. An UAS or other ultimate source of Network RID information feeds an USS acting as a Network RID Service Provider (Net-RID SP), which essentially proxies for

that and other sources; an observer or other ultimate consumer of Network RID information obtains it from a Network RID Display Provider (Net-RID DP), which aggregates information from multiple Net-RID SPs to offer coverage of an airspace volume of interest. Network RID Service and Display providers are expected to be implemented as servers in well-connected infrastructure, accessible via typical means such as web APIs/browsers.

Network RID is the more flexible and less constrained of the defined UAS RID means, but is only partially specified in [F3411-19]. It is presumed that IETF efforts supporting Broadcast RID (see next section) can be easily generalized for Network RID.

3.2. Broadcast RID

[F3411-19] specifies 3 Broadcast RID data links: Bluetooth 4.X; Bluetooth 5.X Long Range; and WiFi with Neighbor Awareness Networking (NAN). For compliance with this standard, an UA must broadcast (using advertisement mechanisms where no other option supports broadcast) on at least one of these; if broadcasting on Bluetooth 5.x, it is also required concurrently to do so on 4.x (referred to in [F3411-19] as Bluetooth Legacy).

The selection of the Broadcast media was driven by research into what is commonly available on 'ground' units (smartphones and tablets) and what was found as prevalent or 'affordable' in UA. Further, there must be an Application Programming Interface (API) for the observer's receiving application to have access to these messages. As yet only Bluetooth 4.X support is readily available, thus the current focus is on working within the 26 byte limit of the Bluetooth 4.X "Broadcast Frame" transmitted on beacon channels. After nominal overheads, this limits the UAS ID string to a maximum length of 20 bytes, and precludes the same frame carrying position, velocity and other information that should be bound to the UAS ID, much less strong authentication data. This requires segmentation ("paging") of longer messages or message bundles ("Message Pack"), and/or correlation of short messages (anticipated by ASTM to be done on the basis of Bluetooth 4 MAC address, which is weak and unverifiable).

3.3. DRIP Focus

DRIP WG will focus on making information obtained via UAS RID immediately usable (for the observer to determine whether the UAS is trusted to fly in the airspace volume where and when observed, to establish communications whereby the observer can inquire of the

pilot as to intent and/or direct the pilot to exit from the volume, etc.):

1. first by making it trustworthy (despite the severe constraints of Broadcast RID);

2. second by enabling verification that an UAS is registered, and if so, in which registry (for classification of trusted operators on the basis of known registry vetting, even by observers lacking Internet connectivity at observation time);

3. third by enabling instant establishment, by authorized parties, of secure communications with the remote pilot.

Any UA can assert any ID using the [F3411-19] required Basic ID message, which lacks any provisions for verification. The Position/Vector message likewise lacks provisions for verification, and does not contain the ID, so must be correlated somehow with a Basic ID message: the developers of [F3411-19] have suggested using the MAC addresses, but these may be randomized by the operating system stack to avoid the adversarial correlation problems of static identifiers. The [F3411-19] optional Authentication Message specifies framing for authentication data, but does not specify any authentication method, and the maximum length of the specified framing is too short for conventional digital signatures and far too short for conventional certificates. The one-way nature of Broadcast RID precludes challenge-response security protocols (e.g. observers sending nonces to UA, to be returned in signed messages). An observer would be seriously challenged to validate the asserted UAS ID or any other information about the UAS or its operator looked up therefrom.

Further, [F3411-19] provides very limited choices for an observer to communicate with the pilot, e.g. to request further information on the UAS operation or exit from an airspace volume in an emergency. The System Message provides the location of the pilot/GCS, so an observer could physically go to the asserted GCS location to look for the remote pilot. An observer with Internet connectivity could look up operator PII in a registry, then call a phone number in hopes someone who can immediately influence the UAS operation will answer promptly during that operation.

Thus complementing [F3411-19] with protocols enabling strong authentication, preserving operator privacy while enabling immediate use of information by authorized parties, is critical to achieve widespread adoption of a RID system supporting safe and secure operation of UAS.

4. Requirements

4.1. General

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).

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.

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.

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.

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

4.2. Identifier

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).

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.

4.3. Privacy

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.

5. IANA Considerations

It is likely that an IPv6 prefix or other namespace will be needed; this will be specified in other documents.

6. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. DRIP information must be divided into 2 classes: that which, to achieve the purpose, must be published openly in clear plaintext, for the benefit of any observer; and that which must be protected (e.g. PII of pilots) but made available to properly authorized parties (e.g. public safety personnel who urgently need to contact pilots in emergencies). Details of the protection mechanisms will be provided in other documents. Classifying the information will be addressed primarily in external standards; herein it will be regarded as a matter for CAA, registry and operator policies, for which enforcement mechanisms will be defined within the scope of DRIP WG and offered. Mitigation of adversarial correlation will also be addressed.

7. Acknowledgments

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM [F3411-19] and IETF DRIP WG efforts. The work of ASTM F38.02 in balancing the interests of diverse stakeholders is essential to the necessary rapid and widespread deployment of UAS RID.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", September 2019.

[Delegated] European Union Aviation Safety Agency (EASA), "Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems", March 2019.

[F3411-19] ASTM, "Standard Specification for Remote ID and Tracking", December 2019.

[Implementing] European Union Aviation Safety Agency (EASA), "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft", May 2019.

[NPRM] United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019.

[Recommendations] FAA UAS Identification and Tracking Aviation Rulemaking Committee, "UAS ID and Tracking ARC Recommendations Final Report", September 2017.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[Stranger] Heinlein, R.A., "Stranger in a Strange Land", June 1961.

Authors' Addresses

Stuart W. Card (editor)
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com