Workgroup: DRIP
Internet-Draft: draft-ietf-drip-reqs-02
Published: 13 July 2020
Intended Status: Informational
Expires: 14 January 2021
Authors: S. Card, Ed. A. Wiethuechter R. Moskowitz
AX Enterprize AX Enterprize HTT Consulting
A. Gurtov
Linköping University

Drone Remote Identification Protocol (DRIP) Requirements

Abstract

This document defines the requirements for Drone Remote Identification Protocol (DRIP) Working Group protocols to support Unmanned Aircraft System Remote Identification and tracking (UAS RID) for security, safety and other purposes. Complementing external technical standards as regulator-accepted means of compliance with UAS RID regulations, DRIP will:

facilitate use of existing Internet resources to support UAS RID and to enable enhanced related services;

enable online and offline verification that UAS RID information is trustworthy.

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 14 January 2021.

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 (Informative)
  1.1. Overall Context
  1.2. Intended Use
  1.3. DRIP Scope
2. Terms and Definitions
  2.1. Requirements Terminology
  2.2. Definitions
3. UAS RID Problem Space
  3.1. Network RID
  3.2. Broadcast RID
  3.3. DRIP Focus
4. Requirements
  4.1. General
  4.2. Identifier
  4.3. Privacy
  4.4. Registries
5. Discussion and Limitations
6. IANA Considerations
7. Security Considerations
8. Privacy and Transparency Considerations
9. References
  9.1. Normative References
  9.2. Informative References
Acknowledgments
Authors' Addresses

1. Introduction (Informative)

1.1. Overall Context

Many considerations (especially safety and security) dictate that UAS be remotely identifiable. Any Observer with responsibilities involving aircraft inherently must classify Unmanned Aircraft (UA) situationally according to basic considerations, as illustrated notionally in Figure 1 below. An Observer who classifies an UAS: as Taskable, can ask it to do something useful; as Low Concern, can reasonably assume it is not malicious, and would cooperate with requests to modify its flight plans for safety reasons; as High Concern or Unidentified, is worth focused surveillance.

```
                     xxxxxxx        +--------------+
                    x       x  No   |              |
                   x   ID?   x+---->| UNIDENTIFIED |
                    x       x       |              |
                     xxxxxxx        +--------------+
                        +
                        | Yes
                        v
                     xxxxxxx
                    x       x
        +---------+x  TYPE?  x+----------+
        |           x       x            |
        |            xxxxxxx             |
        |               +                |
        v               v                v
+--------------+ +--------------+ +--------------+
|              | |              | |              |
|  TASKABLE    | | LOW CONCERN  | | HIGH CONCERN |
|              | |              | |              |
+--------------+ +--------------+ +--------------+
```

Figure 1: "Notional UAS Classification">

Civil Aviation Authorities (CAAs) worldwide are mandating Unmanned Aircraft System Remote Identification and tracking (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] and has described the key role that UAS RID plays in UAS Traffic Management (UTM [CONOPS] especially Section 2.6). CAAs currently (2020) 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 two means of UAS RID:

> Network RID defines a set of information for UAS to make available globally indirectly via the Internet, through servers that can be queried by Observers.

> Broadcast RID defines a set of messages for Unmanned Aircraft (UA) to transmit locally directly one-way over Bluetooth or Wi-Fi, to be received in real time by local Observers.

The same information must be provided via both means. The presentation may differ, as Network RID defines a data dictionary, whereas Broadcast RID defines message formats (which carry items from that same data dictionary). The frequency with which it is sent may differ, as Network RID can accomodate Observer queries asynchronous to UAS updates (which generally need be send only when information, such as position, changes), whereas Broadcast RID depends upon Observers receiving UA messages at the time they are transmitted. Network RID depends upon Internet connectivity in several segments from the UAS to each Observer. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the directly locally received UAS Identifier (UAS ID) as a key.

[F3411-19] specifies three UAS ID types:

TYPE-1 A static, manufacturer assigned, hardware serial number per ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A].

TYPE-2 A CAA assigned (presumably static) ID.

TYPE-3 A 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 as cleartext (ASCII or binary), so static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g., package delivery routes of competitors.

[WG105] addreses a "different scope than Direct Remote Identification... latter being primarily meant for security purposes... rather than for safety purposes (e.g. hazards deconfliction..." Aviation community standards set a higher bar for safety than for security. It "leaves the opportunity for those manufacturers who would prefer to merge both functions to do so... The purpose of the e-Identification function is to transmit, towards the U-space infrastructure and/or other UA, a set of information for safety (traffic management) purposes..." In addition to RID's Broadcast and Network one-way to Observers), it will use V2V to other UA (also perhaps to and/or from some manned aircraft).

1.2. Intended Use

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 (typically 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 Cost, Size, Weight and Power ($SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and Observer receive RID capabilities. $SWaP is a burden not only on the designers of new UA for production and sale, but also on owners of existing UA that must be retrofit. Radio Controlled (RC) aircraft modelers, "hams" who use licensed amateur radio frequencies to control UAS, drone hobbyists and others who custom build UAS all need means of participating in UAS RID sensitive to both generic $SWaP and application-specific considerations.

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.

Despite work by regulators and Standards Development Organizations (SDOs), there are substantial gaps in UAS standards generally and UAS RID specifically. [Roadmap] catalogs UAS related standards, ongoing standardization activities and gaps (as of early 2020); Section 7.8 catalogs those related specifically to UAS RID.

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]) is desirable.

1.3. DRIP Scope

DRIP's initial 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. By "immediately actionable" is meant information of sufficient precision, accuracy, timeliness, etc. for an Observer to use it as the basis for immediate decisive action, whether that be to trigger a defensive counter-UAS system, to attempt to initiate communications with the UAS operator, to accept the presence of the UAS in the airspace where/when observed as not requiring further action, or whatever, with potentially severe consequences of any action or inaction chosen based on that information. Potential follow-on goals may extend beyond providing timely and trustworthy identification data, to using it to enable identity-oriented networking of UAS.

DRIP (originally 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 based architecture for UAS RID conforming to proposed regulations and external technical standards is described in a companion architecture document [drip-architecture] and elaborated in other DRIP documents; this document describes only relevant requirements and defines terminology for the set of DRIP documents.

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

This section defines a set of terms expected to be used in DRIP documents. This list is meant to be the DRIP terminology reference. Some of the terms listed below are not used in this document. [RFC4949] provides a glossary of Internet security terms that should be used where applicable. In the UAS community, the plural form of acronyms generally is the same as the singular form, e.g. Unmanned Aircraft System (singular) and Unmanned Aircraft Systems (plural) are both represented as UAS. On this and other terminological issues, to encourage comprehension necessary for adoption of DRIP by the intended user community, that community's norms are respected herein, and definitions are quoted in cases where they have been found in that community's documents.

$SWaP

Cost, Size, Weight and Power.

AAA

Attestation, Authentication, Authorization, Access Control, Accounting, Attribution, Audit, or any subset thereof (uses differ by application, author and context).

ABDAA

AirBorne DAA. Accomplished using systems onboard the aircraft involved. Also known as "self-separation".

ADS-B

Automatic Dependent Surveillance - Broadcast. "ADS-B Out" equipment obtains aircraft position from other on-board systems (typically GNSS) and periodically broadcasts it to "ADS-B In" equipped entities, including other aircraft, ground stations and satellite based monitoring systems.

AGL

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

ATC

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

ATM

Air Traffic Management. A broader functional and geographic scope and/or a higher layer of abstraction than ATC. "The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management - safely, economically and efficiently - through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions." [ICAOATM]

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.

BLOS

Beyond Line Of Sight (LOS). Term to be avoided due to ambiguity. See LOS.

BVLOS

Beyond Visual Line Of Sight (V-LOS). See V-LOS.

CAA

Civil Aviation Authority. Two examples are the United States Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA).

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. Previously primarily used in military contexts. In the UAS context, typically refers to the link between GCS and UA over which the former controls the latter.

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.

EUROCAE

European Organisation for Civil Aviation Equipment. Aviation SDO, originally European, now with broader membership. Cooperates extensively with RTCA.

GBDAA

Ground Based DAA. Accomplished with the aid of ground based functions.

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.

GNSS

Global Navigation Satellite System. Satellite based timing and/or positioning with global coverage, often used to support navigation.

GPS

Global Positioning System. A specific GNSS, but in this context, the term is typically misused in place of the more generic term GNSS.

GRAIN

Global Resilient Aviation Interoperable Network. Putative ICAO managed IPv6 overlay internetwork per IATF.

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 also for a GCS), measured in or meters.

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. Potentially could provide not only information sent via UAS RID but also information retrieved from UAS RID registries, or information beyond UAS RID, regarding subscribed USS. 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 collects RID messages from UAS and responds to NetRID-DP queries for information on UAS of which it is aware. 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

An entity (typically but not necessarily an individual human) who has directly or indirectly observed an UA and wishes to know something about it, starting with its ID. An observer typically is on the ground and local (within VLOS of an observed UA), but could be remote (observing via Network RID or other surveillance), operating another UA, aboard another aircraft , etc.

Operation

A flight, or series of flights of the same mission, by the same UAS, in the same airspace volume, separated by at most brief ground intervals.

Operator

"A person, organization or enterprise engaged in or offering to engage in an aircraft operation." [ICAOUTM]

Operator ID Message

F3411 Message Type 5. Provides CAA issued Operator ID, only. Operator ID is distinct from UAS ID.

PIC

Pilot In Command. "The pilot designated by the operator, or in the case of general aviation, the owner, as being in command and charged with the safe conduct of a flight." [ICAOATM]

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.

Remote Pilot

A pilot using a GCS to exercise proximate control of an UA. Either the PIC or under the supervision of the PIC.

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.

RTCA

Radio Technical Commission for Aeronautics. US aviation SDO. Cooperates extensively with EUROCAE.

Self-ID Message

F3411 Message Type 3. Provides a 1 byte descriptor and 23 byte ASCII free text field, only. Expected to be used to provide context on the operation, e.g. mission intent.

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.

SDO

Standards Development Organization. ASTM, IETF, et al.

SDSP

Supplemental Data Service Provider. An entity that participates in the UTM system, but provides services beyond those specified as basic UTM system functions. E.g., provides weather data.

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; see Section 1.1, Paragraph 7 for currently defined values.

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. "A USS is an entity that assists UAS Operators with meeting UTM operational requirements that enable safe and efficient use of airspace" and "... provide 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" per [CONOPS].

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/application 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 Wi-Fi, but provided the data link can support at least UDP/IP and ideally also TCP/IP, its type is generally immaterial to the higher layer protocols. An UAS as the 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 three Broadcast RID data links: Bluetooth 4.X; Bluetooth 5.X Long Range; and Wi-Fi with Neighbor Awareness Networking (NAN). For compliance with [F3411-19], 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 will focus on making information obtained via UAS RID immediately usable:

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

2. 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. by facilitating independent reports of UA's aeronautical data (location, velocity, etc.) to confirm or refute the operator self-reports upon which UAS RID and UTM tracking are based;

4. 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), even on an observer device lacking Internet connectivity at the time of observation.

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, 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.

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

GEN-6 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-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 essentially all participating nodes (UA, GCS, Observers, Net-RID SP, Net-RID DP, Private Registry, SDSP).

GEN-9 Multihoming: DRIP MUST support multihoming of UA and GCS, 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.

4.2. Identifier

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.

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.

Note that Registry ID and Entity ID are requirements on a single DRIP entity Identifier, not separate (types of) ID. In the most common use case, the Entity will be the UA, and the DRIP Identifier will be the UAS ID; however, other entities may also benefit from having DRIP identifiers, so the Entity type is not prescribed here.

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. 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.

PRIV-3 Encrypted Storage: DRIP SHOULD facilitate selective strong encryption of private data at rest in such a manner that only authorized actors can recover it.

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.

4.4. Registries

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.

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.

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.

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.

5. Discussion and Limitations

This document is largely based on the process of one SDO, ASTM. Therefore, it is tailored to specific needs and data formats of this standard. Other organizations, for example in EU, do not necessary follow the same architecture. IETF traditionally operates assuming the source material for the standardization process is publicly available. However, ASTM standards require a fee for download. Therefore a double-liaison program at IETF might need to be activated, providing free access to ASTM specifications for contributors to IETF documents.

The need for drone ID and operator privacy is an open discussion topic. For instance, in the ground vehicular domain each car carries a publicly visible plate number. In some countries, for nominal cost or even for free, anyone can resolve the identity and contact information of the owner. Civil commercial aviation and maritime industries also have a tradition of broadcasting plane or ship ID, coordinates and even flight plans in plain text. Community networks such as OpenSky and Flightradar use this open information through ADS-B to deploy public services of flight tracking. Many researchers also use these data to perform optimization of routes and airport operations. Such ID information should be integrity protected, but not necessarily confidential.

In civil aviation, aircraft identity is broadcast by a device known as transponder. It transmits a four-digit squawk code, which is assigned by a traffic controller to an airplane after approving a flight plan. There are several reserved codes such as 7600 which indicate radio communication failure. The codes are unique in each traffic area and can be re-assigned when entering another control area. The code is transmitted in plain text by the transponder and also used for collision avoidance by a system known as Traffic alert and Collision Avoidance System (TCAS). The system could be used for UAS as well initially, but the code space is quite limited and likely to be exhausted soon. The number of UAS far exceeds the number of civil airplanes in operation.

The ADS-B system is utilized in civil aviation for each "ADS-B Out" equipped airplane to broadcast its ID, coordinates and altitude for other airplanes and ground control stations. If this system is adopted for drone IDs, it has additional benefit with backward compatibility with civil aviation infrastructure; then, pilots and dispatchers will be able to see UA on their control screens and take those into account. If not, a gateway translation system between the proposed drone ID and civil aviation system should be implemented. Again, system saturation due to large numbers of UAS is a concern.

Wi-Fi and Bluetooth are two wireless technologies currently recommended by ASTM specifications due to their widespread use and broadcast nature. However, those have limited range (max 100s of meters) and may not reliably deliver UAS ID at high altitude or distance. Therefore, a study should be made of alternative technologies from the telecom domain (WiMax, 5G) or sensor networks (Sigfox, LORA). Such transmission technologies can impose additional restrictions on packet sizes and frequency of transmissions, but could provide better energy efficiency and range. In civil aviation, Controller-Pilot Data Link Communications (CPDLC) is used to transmit command and control between the pilots and ATC. It could be considered for UAS as well due to long range and proven use despite its lack of security [cpdlc].

L-band Digital Aeronautical Communications System (LDACS) is being standardized by ICAO and IETF for use in future civil aviation [I-D.maeurer-raw-ldacs]. It provides secure communication, positioning and control for aircraft using a dedicated radio band. It should be analyzed as a potential provider for UAS RID as well. This will bring the benefit of a global integrated system creating a global airspace use awareness.

6. IANA Considerations

This document does not make any IANA request.

7. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. Potential vulnerabilities of DRIP include but are not limited to:

- Sybil attacks

- Confusion created by many spoofed unsigned messages

- Processing overload induced by attempting to verify many spoofed signed messages (where verification will fail but still consume cycles)

- Malicious or malfunctioning registries

- Interception of (e.g. Man In The Middle attacks on) registration messages

8. Privacy and Transparency Considerations

Privacy is closely related to but not synonomous with security, and conflicts with transparency. Privacy and transparency are important for legal reasons including regulatory consistency. [EU2018] [EU2018]states "harmonised and interoperable national registration systems... should comply with the applicable Union and national law on privacy and processing of personal data, and the information stored in those registration systems should be easily accessible."

Privacy and transparency (where essential to security or safety) are also ethical and moral imperatives. Even in cases where old practices (e.g. automobile registration plates) could be imitated, when new applications involving PII (such as UAS RID) are addressed and newer technologies could enable improving privacy, such opportunities should not be squandered. Thus is is recommended that all DRIP documents give due regard to [RFC6973] and more broadly [RFC8280].

DRIP information falls into two classes: that which, to achieve the purpose, must be published openly as cleartext, for the benefit of any Observer (e.g. the basic UAS ID itself); 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). This classification must be made explicit and reflected with markings, design, etc. 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. Details of the protection mechanisms will be provided in other DRIP documents. Mitigation of adversarial correlation will also be addressed.

9. References

9.1. 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>.

9.2. Informative References

[CONOPS] FAA Office of NextGen, "UTM Concept of Operations v2.0", March 2020.

[cpdlc]
Gurtov, A., Polishchuk, T., and M. Wernberg, "Controller-Pilot Data Link Communication Security", MDPI Sensors 18(5), 1636, 2018, <https://www.mdpi.com/1424-8220/18/5/1636>.

[crowd-sourced-rid]
Moskowitz, R., Card, S., Wiethuechter, A., Zhao, S., and H. Birkholz, "Crowd Sourced Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-crowd-sourced-rid-04, 20 May 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-crowd-sourced-rid-04>.

[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.

[drip-architecture] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-arch-02, 23 June 2020, <https://tools.ietf.org/html/draft-ietf-drip-arch-02>.

[drip-auth] Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Authentication Formats", Work in Progress, Internet-Draft, draft-wiethuechter-drip-auth-01, 10 July 2020, <https://tools.ietf.org/html/draft-wiethuechter-drip-auth-01>.

[drip-identity-claims]
Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Identity Claims", Work in Progress, Internet-Draft, draft-wiethuechter-drip-identity-claims-00, 23 March 2020, <https://tools.ietf.org/html/draft-wiethuechter-drip-identity-claims-00>.

[drip-secure-nrid-c2]
Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "Secure UAS Network RID and C2 Transport", Work in Progress, Internet-Draft, draft-moskowitz-drip-secure-nrid-c2-00, 6 April 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-secure-nrid-c2-00>.

[drip-uas-rid] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-

Draft, draft-moskowitz-drip-uas-rid-02, 28 May 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-uas-rid-02>.

[EU2018] European Parliament and Council, "2015/0277 (COD) PE-CONS 2/18", February 2018.

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

[hhit-registries] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", Work in Progress, Internet-Draft, draft-moskowitz-hip-hhit-registries-02, 9 March 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hhit-registries-02>.

[hierarchical-hit] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-05, 13 May 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-05>.

[I-D.maeurer-raw-ldacs] Maeurer, N., Graeupl, T., and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)", Work in Progress, Internet-Draft, draft-maeurer-raw-ldacs-04, 2 July 2020, <https://tools.ietf.org/html/draft-maeurer-raw-ldacs-04>.

[ICAOATM] International Civil Aviation Organization, "Doc 4444: Procedures for Air Navigation Services: Air Traffic Management", November 2016.

[ICAOUTM] International Civil Aviation Organization, "Unmanned Aircraft Systems Traffic Management (UTM) - A Common Framework with Core Principles for Global Harmonization, Edition 2", November 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.

[new-hip-crypto] Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-04, 23 January 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-new-crypto-04>.

[new-orchid] Moskowitz, R., Card, S., and A. Wiethuechter, "Using cSHAKE in ORCHIDs", Work in Progress, Internet-Draft, draft-moskowitz-orchid-cshake-01, 21 May 2020, <https://tools.ietf.org/html/draft-moskowitz-orchid-cshake-01>.

[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>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[Roadmap] American National Standards Institute (ANSI) Unmanned Aircraft Systems Standardization Collaborative (UASSC), "Standardization Roadmap for Unmanned Aircraft Systems draft v2.0", April 2020.

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

[WG105] European Parliament and Council, "EUROCAE WG-105 draft Minimum Operational Performance Standards (MOPS) for Unmanned Aircraft System (UAS) Electronic Identification"", June 2020.

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 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. IETF volunteers who have contributed to this draft include Amelia Andersdotter, Mohamed Boucadair, Toerless Eckert, Susan Hares, Mika J&#228;rvenp&#228;&#228;, Daniel Migault, Saulo Da Silva and Shuai Zhao.

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

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping
Sweden

Email: gurtov@acm.org