Internet Engineering Task Force (IETF)
Request for Comments: 9153
Category: Informational
ISSN: 2070-1721

S. Card, Ed.
A. Wiethuechter
AX Enterprize
R. Moskowitz
HTT Consulting
A. Gurtov
Linköping University

February 2022

Drone Remote Identification Protocol (DRIP) Requirements and Terminology

Abstract

This document defines terminology and requirements for solutions produced by the Drone Remote Identification Protocol (DRIP) Working Group. These solutions will support Unmanned Aircraft System Remote Identification and tracking (UAS RID) for security, safety, and other purposes (e.g., initiation of identity-based network sessions supporting UAS applications). DRIP will facilitate use of existing Internet resources to support RID and to enable enhanced related services, and it will enable online and offline verification that RID information is trustworthy.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9153.

1. Introduction

This document defines terminology and requirements for solutions produced by the Drone Remote Identification Protocol (DRIP) Working Group. These solutions will support Unmanned Aircraft System Remote Identification and tracking (UAS RID) for security, safety, and other purposes (e.g., initiation of identity-based network sessions supporting UAS applications). DRIP will facilitate use of existing Internet resources to support RID and to enable enhanced related services, and it will enable online and offline verification that RID information is trustworthy.

For any unfamiliar or a priori ambiguous terminology herein, see Section 2.

1.1. Motivation and External Influences

Many considerations (especially safety and security) necessitate Unmanned Aircraft System Remote Identification and tracking (UAS

RID).

Unmanned Aircraft (UA) may be fixed-wing, rotary-wing (e.g., helicopter), hybrid, balloon, rocket, etc. Small fixed-wing UA typically have Short Take-Off and Landing (STOL) capability; rotary-wing and hybrid UA typically have Vertical Take-Off and Landing (VTOL) capability. UA may be single- or multi-engine. The most common today are multicopters (rotary-wing, multi-engine). The explosion in UAS was enabled by hobbyist development of advanced flight stability algorithms for multicopters that enabled even inexperienced pilots to take off, fly to a location of interest, hover, and return to the takeoff 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 Navigation Satellite System (GNSS) waypoint to waypoint in a weak form of autonomy; stronger autonomy is coming.

Small UA are "low observable" as they:

* typically have small radar cross sections;

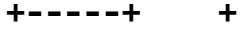
* make noise that is quite noticeable at short ranges but difficult to detect at distances they can quickly close (500 meters in under 13 seconds by the fastest consumer mass-market drones available in early 2021);

* typically fly at low altitudes (e.g., under 400 feet Above Ground Level (AGL) for UA to which RID applies in the US, as per [Part107]); and

* are highly maneuverable and thus can fly under trees and between buildings.

UA can carry payloads (including sensors, cyber weapons, 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.

Diverse other applications can be enabled or facilitated by RID. Internet protocols typically start out with at least one entity already knowing an identifier or locator of another; but an entity (e.g., UAS or Observer device) encountering an a priori unknown UA in physical space has no identifier or logical space locator for that UA, unless and until one is provided somehow. RID provides an identifier, which, if well chosen, can facilitate use of a variety of Internet family protocols and services to support arbitrary applications beyond the basic security functions of RID. For most of these, some type of identifier is essential, e.g., Network Access Identifier (NAI), Digital Object Identifier (DOI), Uniform Resource Identifier (URI), domain name, or public key. DRIP motivations include both the basic security and the broader application support functions of RID. The general scenario is illustrated in Figure 1.



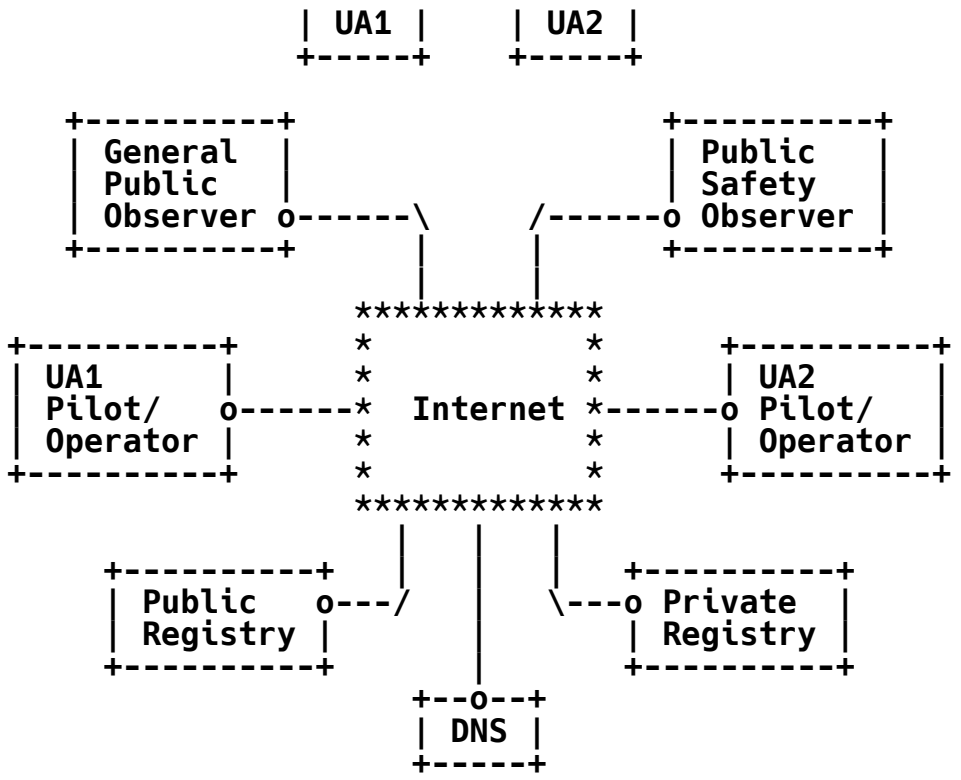


Figure 1: General UAS RID Usage Scenario

Figure 1 illustrates a typical case where there may be the following:

* multiple Observers, some of them members of the general public and others government officers with public safety and security responsibilities,

* multiple UA in flight within observation range, each with its own pilot/operator,

* at least one registry each for lookup of public and (by authorized parties only) private information regarding the UAS and their pilots/operators, and

* in the DRIP vision, DNS resolving various identifiers and locators of the entities involved.

Note the absence of any links to/from the UA in the figure; this is because UAS RID and other connectivity involving the UA varies. Some connectivity paths do or do not exist depending upon the scenario. Command and Control (C2) from the Ground Control Station (GCS) to the UA via the Internet (e.g., using LTE cellular) is expected to become much more common as Beyond Visual Line Of Sight (BVLOS) operations increase; in such a case, there is typically not also a direct wireless link between the GCS and UA. Conversely, if C2 is running over a direct wireless link, then the GCS typically has Internet connectivity, but the UA does not. Further, paths that nominally exist, such as between an Observer device and the Internet, may be severely intermittent. These connectivity constraints are likely to have an impact, e.g., on how reliably DRIP requirements can be

satisfied.

An Observer of UA may need to classify them, as illustrated notionally in Figure 2, for basic airspace Situational Awareness (SA). An Observer can classify a UAS as one of the following and treat as:

* Taskable: can ask it to do something useful.

* Low Concern: can reasonably assume it is not malicious and would cooperate with requests to modify its flight plans for safety concerns that arise.

* High Concern or Unidentified: can focus surveillance on it.

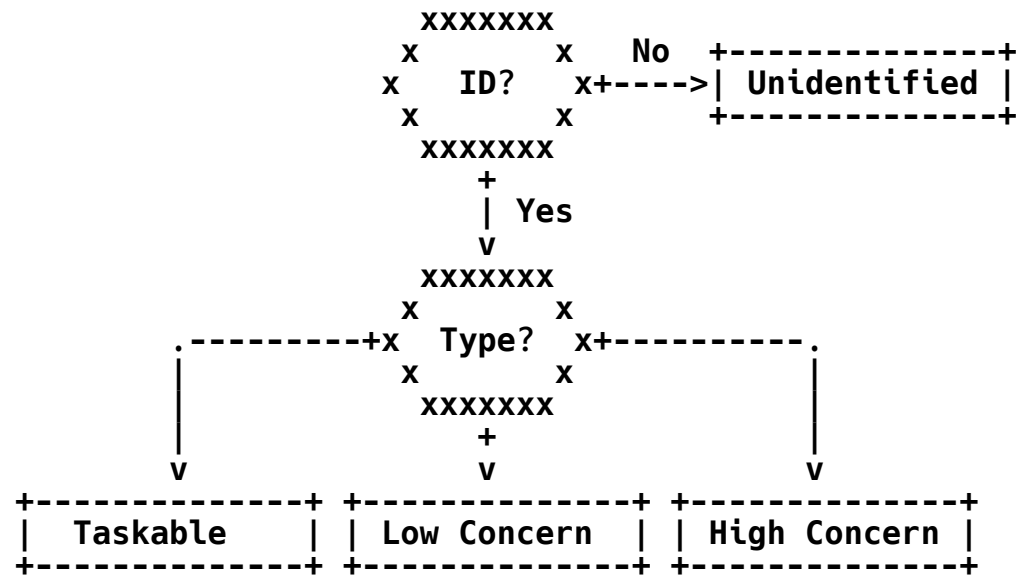


Figure 2: Notional UAS Classification

The widely cited "Standard Specification for Remote ID and Tracking" [F3411-19] was developed by ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041. The published standard is available for purchase from ASTM and is also available as an ASTM membership premium; early draft versions are freely available as Open Drone ID specifications [OpenDroneID]. [F3411-19] is frequently referenced in DRIP, where building upon its link layers and both enhancing support for and expanding the scope of its applications are central foci.

In many applications, including UAS RID, identification and identifiers are not ends in themselves; they exist to enable lookups and provision of other services.

Using UAS RID to facilitate vehicular (i.e., Vehicle-to-Everything (V2X)) communications and applications such as Detect And Avoid (DAA), which would impose tighter latency bounds than RID itself, is an obvious possibility; this is explicitly contemplated in the "Remote Identification of Unmanned Aircraft" rule of the US Federal Aviation Administration (FAA) [FRUR]. However, usage of RID systems

and information beyond mere identification (primarily to hold operators accountable after the fact), including DAA, were declared out of scope in ASTM F38.02 WK65041, based on a distinction between RID as a security standard versus DAA as a safety application. Standards Development Organizations (SDOs) in the aviation community generally set a higher bar for safety than for security, especially with respect to reliability. Each SDO has its own cultural set of connotations of safety versus security; the denotative definitions of the International Civil Aviation Organization (ICAO) are cited in Section 2.

[Opinion1] and [WG105] cite the Direct Remote Identification (DRI) previously required and specified, explicitly stating that whereas DRI is primarily for security purposes, the "Network Identification Service" [Opinion1] (in the context of U-space [InitialView]) or "Electronic Identification" [WG105] is primarily for safety purposes (e.g., Air Traffic Management, especially hazards deconfliction) and also is allowed to be used for other purposes such as support of efficient operations. These emerging standards allow the security- and safety-oriented systems to be separate or merged. In addition to mandating both Broadcast and Network RID one-way to Observers, they will use Vehicle-to-Vehicle (V2V) to other UAS (also likely to and/or from some manned aircraft). These reflect the broad scope of the European Union (EU) U-space concept, as being developed in the Single European Sky ATM Research (SESAR) Joint Undertaking, the U-space architectural principles of which are outlined in [InitialView].

ASD-STAN is an Associated Body to CEN (European Committee for Standardization) for Aerospace Standards. It has published an EU standard titled "Aerospace series - Unmanned Aircraft Systems - Part 002: Direct Remote Identification" [ASDSTAN4709-002]; a current (early 2021) informal overview is freely available in [ASDRI] (note that [ASDRI] may not precisely reflect the final standard as it was published before [ASDSTAN4709-002]). It will provide compliance to cover the identical DRI requirements applicable to drones of the following classes:

* C1 ([Delegated], Part 2)

* C2 ([Delegated], Part 3)

* C3 ([Delegated], Part 4)

* C5 ([Amended], Part 16)

* C6 ([Amended], Part 17)

The standard contemplated in [ASDRI] will provide UA capability to be identified in real time during the whole duration of the flight, without specific connectivity or ground infrastructure link, utilizing existing mobile devices within broadcast range. It will use Bluetooth 4, Bluetooth 5, Wi-Fi Neighbor Awareness Networking (NAN) (also known as "Wi-Fi Aware" [WiFiNAN]), and/or IEEE 802.11 Beacon modes. The emphasis of the EU standard is compatibility with [F3411-19], although there are differences in mandatory and optional message types and fields.

The DRI system contemplated in [ASDRI] will broadcast the following locally:

1. the UAS operator registration number;

2. the [CTA2063A]-compliant unique serial number of the UA;

3. a time stamp, the geographical position of the UA, and its height AGL or above its takeoff point;

4. the UA ground speed and route course measured clockwise from true north;

5. the geographical position of the Remote Pilot, or if that is not available, the geographical position of the UA takeoff point; and

6. for classes C1, C2, C3, the UAS emergency status.

Under the standard contemplated in [ASDRI], data will be sent in plaintext, and the UAS operator registration number will be represented as a 16-byte string including the (European) state code. The corresponding private ID part will contain three characters that are not broadcast but used by authorities to access regional registration databases for verification.

ASD-STAN also contemplates corresponding Network Remote Identification (NRI) functionality. ASD-STAN plans to revise their current standard with additional functionality (e.g., DRIP) to be published no later than 2022 [ASDRI].

Security-oriented UAS RID essentially has two goals: 1) enable the general public to obtain and record an opaque ID for any observed UA, which they can then report to authorities and 2) enable authorities, from such an ID, to look up information about the UAS and its operator. Safety-oriented UAS RID has stronger requirements.

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 [Recommendations]; however, aside from DRIP, it is not addressed in any of the subsequent regulations or international SDO technical specifications known to the authors as of early 2021.

1.2. Concerns and Constraints

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.

The origin of information in UAS RID and UAS Traffic Management (UTM) generally is the UAS or its operator. Self-reports may be initiated by the Remote Pilot at the console of the GCS (the UAS subsystem used to remotely operate the UA) or automatically by GCS software; in Broadcast RID, they are typically initiated automatically by a process on the UA. Data in the reports may come from sensors

available to the operator (e.g., radar or cameras), the GCS (e.g., "dead reckoning" UA location, starting from the takeoff location and estimating the displacements due to subsequent piloting commands, wind, etc.), or the UA itself (e.g., an on-board GNSS receiver). In Broadcast RID, all the data must be sent proximately by the UA, and most of the data ultimately comes from the UA. Whether information comes proximately from the operator or from automated systems configured by the operator, there are possibilities of unintentional error in and intentional falsification of this data. Mandating UAS RID, specifying data elements required to be sent, monitoring compliance, and enforcing compliance (or penalizing non-compliance) are matters for Civil Aviation Authorities (CAAs) and potentially other authorities. Specifying message formats and supporting technologies to carry those data elements has been addressed by other SDOs. Offering technical means, as extensions to external standards, to facilitate verifiable compliance and enforcement/monitoring is an opportunity for DRIP.

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 in accordance with applicable 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], the basis for most current (2021) thinking about and efforts to provide UAS RID, 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 are not specified therein.

The need for nearly universal deployment of UAS RID is pressing: consider how negligible the value of an automobile license plate system would be if only 90% of the cars displayed plates. This implies the need to support use by Observers of already-ubiquitous mobile devices (typically smartphones and tablets). Anticipating 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 unpaired state requires use of the extremely short BT4 "advertisement" (beacon) frames.

Wireless data links to or from UA are challenging. Flight is often amidst structures and foliage at low altitudes over varied terrain. UA are constrained in both total energy and instantaneous power by their batteries. Small UA imply small antennas. Densely populated volumes will suffer from link congestion: even if UA in an airspace volume are few, other transmitters nearby on the ground, sharing the same license free spectral band, may be many. Thus, air-to-air and air-to-ground links will generally be slow and unreliable.

UAS Cost, Size, Weight, and Power (CSWaP) constraints are severe. CSWaP is a burden not only on the designers of new UAS for sale but also on owners of existing UAS 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 that are sensitive to both generic CSWaP and application-specific considerations.

To accommodate the most severely constrained cases, all of the concerns described above conspire to motivate system design decisions that complicate the protocol design problem.

Broadcast RID uses one-way local data links. UAS may have Internet connectivity only intermittently, or not at all, during flight.

Internet-disconnected operation of Observer devices has been deemed by ASTM F38.02 as too infrequent to address. However, the preamble to [FRUR] cites "remote and rural areas that do not have reliable Internet access" as a major reason for requiring Broadcast rather than Network RID. [FRUR] also states:

> Personal wireless devices that are capable of receiving 47 CFR part 15 frequencies, such as smart phones, tablets, or other similar commercially available devices, will be able to receive broadcast remote identification information directly without reliance on an Internet connection.

Internet-disconnected operation presents challenges, e.g., for Observers needing access to the [F3411-19] web-based Broadcast Authentication Verifier Service or needing to do external lookups.

As RID must often operate within these constraints, heavyweight cryptographic security protocols or even simple cryptographic handshakes are infeasible, yet trustworthiness of UAS RID information is essential. Under [F3411-19], _even the most basic datum, the UAS ID itself, can be merely an unsubstantiated claim_.

Observer devices are ubiquitous; thus, they are popular targets for malware or other compromise, so they 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.

Despite work by regulators and 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 2020); Section 7.8 catalogs those related specifically to UAS RID. DRIP will address the most fundamental of these gaps, as foreshadowed above.

1.3. DRIP Scope

DRIP's initial objective is to make RID immediately actionable, especially in emergencies, in severely constrained UAS environments (both Internet and local-only connected scenarios), balancing legitimate (e.g., public safety) authorities' Need To Know trustworthy information with UAS operators' privacy. The phrase "immediately actionable" means information of sufficient precision,

accuracy, and timeliness for an Observer to use it as the basis for immediate decisive action (e.g., triggering a defensive counter-UAS system, attempting to initiate communications with the UAS operator, accepting the presence of the UAS in the airspace where/when observed as not requiring further action, etc.) with potentially severe consequences of any action or inaction chosen based on that information. For further explanation of the concept of immediate actionability, see [ENISACSIRT].

Note that UAS RID must achieve nearly universal adoption, but DRIP can add value even if only selectively deployed. Authorities with jurisdiction over more sensitive airspace volumes may set a RID requirement, for flight in such volumes, that is higher than generally mandated. Those with a greater need for high-confidence IFF can equip with DRIP, enabling strong authentication of their own aircraft and allied operators without regard for the weaker (if any) authentication of others.

DRIP (originally "Trustworthy Multipurpose Remote Identification (TM-RID)") could be applied to verifiably identify other types of registered things reported to be in specified physical locations. Providing timely trustworthy identification data is also prerequisite to identity-oriented networking. Despite the value of DRIP to these and other potential applications, UAS RID is the urgent motivation and clear initial focus of DRIP. Existing Internet resources (protocol standards, services, infrastructure, and business models) should be leveraged.

1.4. Document Scope

This document describes the problem space for UAS RID conforming to proposed regulations and external technical standards, defines common terminology, specifies numbered requirements for DRIP, identifies some important considerations (security, privacy, and transparency), and discusses limitations.

A natural Internet-based approach to meet these requirements is described in a companion architecture document [DRIP-ARCH] and elaborated in other 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 non-comprehensive set of terms expected to be used in DRIP documents. This list is meant to be the DRIP terminology reference; as such, some of the terms listed below are not used in this document.

To encourage comprehension necessary for adoption of DRIP by the intended user community, the UAS community's norms are respected herein, and definitions are quoted in cases where they have been found in that community's documents. Most of the terms listed below are from that community (even if specific source documents are not cited); any terms that are DRIP-specific or defined by this document are marked "(DRIP)".

Note that, in the UAS community, the plural form of an acronym, generally, is the same as the singular form, e.g., Unmanned Aircraft System (singular) and Unmanned Aircraft Systems (plural) are both represented as UAS.

[RFC4949] provides a glossary of Internet security terms that should be used where applicable.

4-D
: Four-dimensional. Latitude, Longitude, Altitude, Time. Used especially to delineate an airspace volume in which an operation is being or will be conducted.

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

ABDAA
: AirBorne DAA. Accomplished using systems onboard the aircraft involved. Supports "self-separation" (remaining "well clear" of other aircraft) and collision avoidance.

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 a UA, measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (GNSS) altitude.

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. [ICAOATM] defines ATM as the following: "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".

Authentication Message
: [F3411-19] Message Type 2. Provides framing for authentication data only; the only message that can be extended in length by segmenting it across more than one page.

Basic ID Message
: [F3411-19] Message Type 0. Provides UA Type, ID Type (and Specific Session ID subtype if applicable), and UAS ID only.

Broadcast Authentication Verifier Service
: System component designed to handle any authentication of Broadcast RID by offloading signature verification to a web service [F3411-19].

BVLOS
: Beyond Visual Line Of Sight. See VLOS.

byte
: Used here in its now-customary sense as a synonym for "octet", as "byte" is used exclusively in definitions of data structures specified in [F3411-19].

CAA
: Civil Aviation Authority of a regulatory jurisdiction. Often so named, but other examples include the United States Federal Aviation Administration (FAA) and the Japan Civil Aviation Bureau.

CSWaP
: Cost, Size, Weight, and Power

C2
: Command and Control. Previously mostly used in military contexts. Properly refers to a function that is exercisable over arbitrary communications, but in the small UAS context, often refers to the communications (typically RF data link) over which the GCS controls the UA.

DAA
: Detect And Avoid, formerly "Sense And Avoid (SAA)". A means of keeping aircraft "well clear" of each other and obstacles for safety. [ICAOUAS] defines DAA as the following: "The capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action to comply with the applicable rules of flight".

DRI (not to be confused with DRIP)
: Direct Remote Identification. EU regulatory requirement for "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" [Delegated]. This requirement can presumably be satisfied with appropriately configured [F3411-19] Broadcast RID.

DSS
: Discovery and Synchronization Service. The UTM system overlay network backbone. Most importantly, it enables one USS to learn which other USS have UAS operating in a given 4-D airspace volume, for strategic deconfliction of planned operations and Network RID surveillance of active operations. See [F3411-19].

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 GNSS waypoints, or by 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 the UAS context, the term is typically misused in place of the more generic term "GNSS".

GRAIN
: Global Resilient Aviation Interoperable Network. ICAO-managed IPv6 overlay internetwork based on IATF that is dedicated to aviation (but not just aircraft). As currently (2021) designed, it accommodates the proposed DRIP identifier.

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 specialized agency of the United Nations that develops and harmonizes international standards relating to aviation.

IFF
: Identification Friend or Foe. Originally, and in its narrow sense still, a self-identification broadcast in response to interrogation via radar to reduce friendly fire incidents, which led to military and commercial transponder systems such as ADS-B. In the broader sense used here, any process intended to distinguish friendly from potentially hostile UA or other entities encountered.

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. FAA-authorized partial stopgap in the US until UTM comes.

Location/Vector Message
: [F3411-19] Message Type 1. Provides UA location, altitude, heading, speed, and status.

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 VLOS.

Message Pack
: [F3411-19] Message Type 15. The framed concatenation, in message type index order, of at most one message of each type of any subset of the other types. Required to be sent in Wi-Fi NAN and in Bluetooth 5 Extended Advertisements, if those media are used; cannot be sent in Bluetooth 4.

MSL
: Mean Sea Level. Shorthand for relative altitude, above the variously defined mean sea level, typically of a UA (but in [FRUR], also for a GCS), measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (e.g., as indicated by GNSS, referenced to the WGS84 ellipsoid).

Net-RID DP
: Network RID Display Provider. [F3411-19] 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. Under superseded [NPRM], not recognized as a distinct entity, but as 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. [F3411-19] logical entity that collects RID messages from UAS and responds to Net-RID DP queries for information on UAS of which it is aware. Under superseded [NPRM], the USS to which the UAS is subscribed (i.e., the "Remote ID USS").

Network Identification Service
: EU regulatory requirement in [Opinion1], corresponding to the Electronic Identification for which Minimum Operational Performance Standards are specified in [WG105], which presumably

can be satisfied with appropriately configured [F3411-19] Network RID.

Observer
: An entity (typically, but not necessarily, an individual human) who has directly or indirectly observed a 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. (DRIP)

Operation
: A flight, or series of flights of the same mission, by the same UAS, separated by, at most, brief ground intervals. (Inferred from UTM usage; no formal definition found.)

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

Operator ID Message
: [F3411-19] Message Type 5. Provides CAA-issued Operator ID only. Operator ID is distinct from UAS ID.

page
: Payload of a frame, containing a chunk of a message that has been segmented, that allows transport of a message longer than can be encapsulated in a single frame. See [F3411-19].

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" [ICAOUAS].

PII
: Personally Identifiable Information. In the UAS RID context, typically of the UAS Operator, PIC, or Remote Pilot, but possibly of an Observer or other party. This specific term is used primarily in the US; other terms with essentially the same meaning are more common in other jurisdictions (e.g., "personal data" in the EU). Used herein generically to refer to personal information that the person might wish to keep private or may have a statutorily recognized right to keep private (e.g., under the EU [GDPR]), potentially imposing (legally or ethically) a confidentiality requirement on protocols/systems.

Remote Pilot
: A pilot using a GCS to exercise proximate control of a UA. Either the PIC or under the supervision of the PIC. "The person who manipulates the flight controls of a remotely-piloted aircraft during flight time" [ICAOUAS].

RF
: Radio Frequency. Can be used as an adjective (e.g., "RF link") or as a noun.

RF LOS
RF Line Of Sight. Typically used in describing 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 VLOS.

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

Safety
"The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level" (from Annex 19 of the Chicago Convention, quoted in [ICAODEFS]).

Security
"Safeguarding civil aviation against acts of unlawful interference" (from Annex 17 of the Chicago Convention, quoted in [ICAODEFS]).

Self-ID Message
[F3411-19] 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.

SDO
Standards Development Organization, such as ASTM, IETF, etc.

SDSP
Supplemental Data Service Provider. An entity that participates in the UTM system but provides services (e.g., weather data) beyond those specified as basic UTM system functions. See [FAACONOPS].

System Message
[F3411-19] 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 types of airspace, including but not limited to volumes that are in high-density urban areas and/or shared with manned aircraft [InitialView].

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

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 [F3411-19].

UAS ID
: UAS identifier. Although called "UAS ID", it is actually unique to the UA, neither to the operator (as some UAS registration numbers have been and for exclusively recreational purposes are continuing to be assigned), nor to the combination of GCS and UA that comprise the UAS. _Maximum length of 20 bytes_ [F3411-19]. If the ID Type is 4, the proposed Specific Session ID, then the 20 bytes includes the subtype index, leaving only 19 bytes for the actual identifier.

ID Type
: UAS identifier type index. 4 bits. See Section 3, Paragraph 6 for current standard values 0-3 and currently proposed additional value 4. See also [F3411-19].

UAS RID
: UAS Remote Identification and tracking. System to enable arbitrary Observers to identify UA during flight.

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" [FAACONOPS]. In addition, "USSs 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" [FAACONOPS].

UTM
: UAS Traffic Management. "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" [ICAOUTM]. In the US, according to the FAA, a "traffic management" ecosystem for "uncontrolled" UAS operations at low altitudes, separate from, but complementary to, the FAA's ATC system for "controlled" operations of manned aircraft.

V2V
: Vehicle-to-Vehicle. Originally communications between automobiles, now extended to apply to communications between vehicles generally. Often, together with Vehicle-to-Infrastructure (V2I) and similar functions, generalized to V2X.

VLOS
: Visual Line Of Sight. Typically used in describing operation of a UA by a "remote" pilot who can clearly and directly (without video cameras or any 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

CAAs worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] regulations. The US FAA has published a "final" rule [FRUR] and has described the key role that UAS RID plays in UAS Traffic Management (UTM) in [FAACONOPS] (especially Section 2.6). At the time of writing, CAAs promulgate performance-based regulations that do not specify techniques but rather cite industry consensus technical standards as acceptable means of compliance.

The most widely cited such industry consensus technical standard for UAS RID is [F3411-19], which 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 UA to transmit locally directly one-way over Bluetooth or Wi-Fi (without IP or any other protocols between the data link and application layers), to be received in real time by local Observers.

UAS using both means must send the same UAS RID application-layer information via each [F3411-19]. 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 interval (or rate) at which it is sent may differ, as Network RID can accommodate Observer queries asynchronous to UAS updates (which generally need be sent only when information, such as location, 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 to retrieve registry information, using, as the primary unique key for database lookup, the UAS Identifier (UAS ID) that was directly locally received. Broadcast RID does not assume IP connectivity of UAS; messages are encapsulated by the UA _without IP_, directly in link-layer frames (Bluetooth 4, Bluetooth 5, Wi-Fi NAN, IEEE 802.11 Beacon, or perhaps others in the future).

[F3411-19] specifies three ID Type values, and its proposed revision (at the time of writing) adds a fourth:

1 A static, manufacturer-assigned, hardware serial number as defined in "Small Unmanned Aerial Systems Serial Numbers" [CTA2063A].

2 A CAA-assigned (generally static) ID, like the registration number of a manned aircraft.

3 A UTM-system-assigned Universally Unique Identifier (UUID) [RFC4122], which can but need not be dynamic.

4 A Specific Session ID, of any of an 8-bit range of subtypes defined external to ASTM and registered with ICAO, for which subtype 1 has been reserved by ASTM for the DRIP entity ID.

Per [Delegated], the EU allows only ID Type 1. Under [FRUR], the US allows ID Type 1 and ID Type 3. [NPRM] proposed that a "Session ID" would be "e.g., a randomly-generated alphanumeric code assigned by a Remote ID UAS Service Supplier (USS) on a per-flight basis designed to provide additional privacy to the operator", but given the omission of Network RID from [FRUR], how this is to be assigned in the US is still to be determined.

As yet, there are apparently no CAA public proposals to use ID Type 2. In the preamble of [FRUR], the FAA argues that registration numbers should not be sent in RID, insists that the capability of looking up registration numbers from information contained in RID should be restricted to FAA and other Government agencies, and implies that Session ID would be linked to the registration number only indirectly via the serial number in the registration database. The possibility of cryptographically blinding registration numbers, such that they can be revealed under specified circumstances, does not appear to be mentioned in applicable regulations or external technical standards.

Per [Delegated], the EU also requires an operator registration number (an additional identifier distinct from the UAS ID) that can be carried in an [F3411-19] optional Operator ID Message.

[FRUR] allows RID requirements to be met either by the UA itself, which is then designated a "standard remote identification unmanned aircraft", or by an add-on "remote identification broadcast module". The requirements for a module are different than for a standard RID UA. The module:

* must transmit its own serial number (neither the serial number of the UA to which it is attached, nor a Session ID),

* must transmit takeoff location as a proxy for the location of the pilot/GCS,

* need not transmit UA emergency status, and

* is allowed to be used only for operations within VLOS of the Remote Pilot.

Jurisdictions may relax or waive RID requirements for certain operators and/or under certain conditions. For example, [FRUR] allows operators with UAS not equipped for RID to conduct VLOS operations at counterintuitively named "FAA-Recognized Identification Areas (FRIAs)"; radio-controlled model aircraft flying clubs and other eligible organizations can apply to the FAA for such recognition of their operating areas.

3.1. Network RID

Figure 3 illustrates Network RID information flows. Only two of the three typically wireless links shown involving the UAS (UA-GCS, UA-Internet, and GCS-Internet) need exist to support C2 and Network RID. All three may exist, at the same or different times, especially in

BVLOS operations. There must be at least one information flow path (direct or indirect) between the GCS and the UA, for the former to exercise C2 over the latter. If this path is two-way (as increasingly it is, even for inexpensive small UAS), the UA will also send its status (and position, if suitably equipped, e.g., with GNSS) to the GCS. There also must be a path between at least one subsystem of the UAS (UA or GCS) and the Internet, for the former to send status and position updates to its USS (serving inter alia as a Net-RID SP).

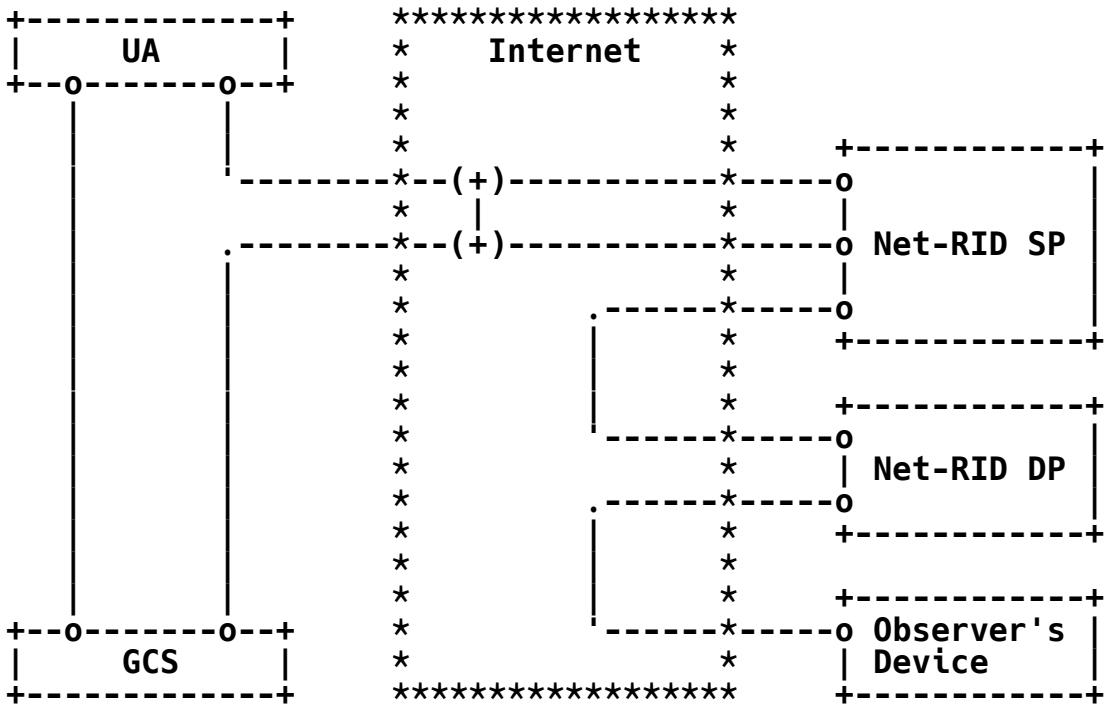


Figure 3: Network RID Information Flow

Direct UA-Internet wireless links are expected to become more common, especially on larger UAS, but, at the time of writing, they are rare. Instead, the RID data flow typically originates on the UA and passes through the GCS, or it originates on the GCS. Network RID data makes three trips through the Internet (GCS-SP, SP-DP, DP-Observer, unless any of them are colocated), implying use of IP (and other middle-layer protocols, e.g., TLS/TCP or DTLS/UDP) on those trips. IP is not necessarily used or supported on the UA-GCS link (if indeed that direct link exists, as it typically does now, but in BVLOS operations often will not).

Network RID is publish-subscribe-query. In the UTM context:

1. The UAS operator pushes an "operational intent" (the current term in UTM corresponding to a flight plan in manned aviation) to the USS (call it USS#1) that will serve that UAS (call it UAS#1) for that operation, primarily to enable deconfliction with other operations potentially impinging upon that operation's 4-D airspace volume (call it Volume#1).

2. Assuming the operation is approved and commences, UAS#1

periodically pushes location/status updates to USS#1, which serves inter alia as the Network RID Service Provider (Net-RID SP) for that operation.

3. When users of any other USS (whether they be other UAS operators or Observers) develop an interest in any 4-D airspace volume (e.g., because they wish to submit an operational intent or because they have observed a UA), they query their own USS on the volumes in which they are interested.

4. Their USS query, via the UTM Discovery and Synchronization Service (DSS), all other USS in the UTM system and learn of any USS that have operations in those volumes (including any volumes intersecting them); thus, those USS whose query volumes intersect Volume#1 (call them USS#2 through USS#n) learn that USS#1 has such operations.

5. Interested parties can then subscribe to track updates on that operation of UAS#1, via their own USS, which serve as Network RID Display Providers (Net-RID DPs) for that operation.

6. USS#1 (as Net-RID SP) will then publish updates of UAS#1 status and position to all other subscribed USS in USS#2 through USS#n (as Net-RID DP).

7. All Net-RID DP subscribed to that operation of UAS#1 will deliver its track information to their users who subscribed to that operation of UAS#1 (via means unspecified by [F3411-19], etc., but generally presumed to be web browser based).

Network RID has several connectivity scenarios:

* _Persistently Internet-connected UA_ can consistently directly source RID information; this requires wireless coverage throughout the intended operational airspace volume, plus a buffer (e.g., winds may drive the UA out of the volume).

* _Intermittently Internet-connected UA_, can usually directly source RID information, but when offline (e.g., due to signal blockage by a large structure being inspected using the UAS), need the GCS to proxy source RID information.

* _Indirectly connected UA_ lack the ability to send IP packets that will be forwarded into and across the Internet but instead have some other form of communications to another node that can relay or proxy RID information to the Internet; typically, this node would be the GCS (which to perform its function must know where the UA is, although C2 link outages do occur).

* _Non-connected UA_ have no means of sourcing RID information, in which case the GCS or some other interface available to the operator must source it. In the extreme case, this could be the pilot or other agent of the operator using a web browser or application to designate, to a USS or other UTM entity, a time-bounded airspace volume in which an operation will be conducted. This is referred to as a "non-equipped network participant"

engaging in "area operations". This may impede disambiguation of ID if multiple UAS operate in the same or overlapping 4-D volumes. In most airspace volumes, most classes of UA will not be permitted to fly if non-connected.

In most cases in the near term (2021), the Network RID first-hop data link is likely to be either cellular (which can also support BVLOS C2 over existing large coverage areas) or Wi-Fi (which can also support Broadcast RID). However, provided the data link can support at least UDP/IP and ideally also TCP/IP, its type is generally immaterial to higher-layer protocols. The UAS, as the ultimate source of Network RID information, feeds a Net-RID SP (typically the USS to which the UAS operator subscribes), which proxies for the UAS and other data sources. An Observer or other ultimate consumer of Network RID information obtains it from a Net-RID DP (also typically a USS), which aggregates information from multiple Net-RID SPs to offer airspace Situational Awareness (SA) coverage of a volume of interest. Network RID Service and Display Providers are expected to be implemented as servers in well-connected infrastructure, communicating with each other via the Internet and accessible by Observers via means such as web Application Programming Interfaces (APIs) and browsers.

Network RID is the less constrained of the defined means of UAS RID. [F3411-19] only specifies information exchanges from Net-RID SP to Net-RID DP. It is presumed that IETF efforts supporting the more constrained Broadcast RID (see next section) can be generalized for Network RID and potentially also for UAS-to-USS or other UTM communications.

3.2. Broadcast RID

Figure 4 illustrates the Broadcast RID information flow. Note the absence of the Internet from the figure. This is because Broadcast RID is one-way direct transmission of application-layer messages over an RF data link (without IP) from the UA to local Observer devices. Internet connectivity is involved only in what the Observer chooses to do with the information received, such as verify signatures using a web-based Broadcast Authentication Verifier Service and look up information in registries using the UAS ID as the primary unique key.

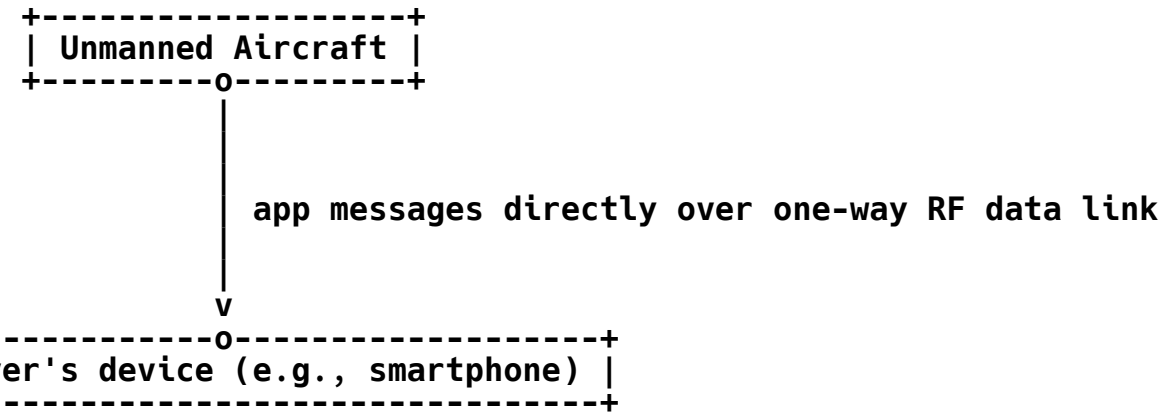


Figure 4: Broadcast RID Information Flow

Broadcast RID is conceptually similar to Automatic Dependent Surveillance - Broadcast (ADS-B). However, for various technical and other reasons, regulators including the EASA have not indicated intent to allow, and FAA has explicitly prohibited, use of ADS-B for UAS RID.

[F3411-19] specifies four Broadcast RID data links: Bluetooth 4.x, Bluetooth 5.x with Extended Advertisements and Long-Range Coded PHY (S=8), Wi-Fi NAN at 2.4 GHz, and Wi-Fi NAN at 5 GHz. A UA must broadcast (using advertisement mechanisms where no other option supports broadcast) on at least one of these. If sending on Bluetooth 5.x, it is required to do so concurrently on 4.x (referred to in [F3411-19] as "Bluetooth Legacy"); current (2021) discussions in ASTM F38.02 on revising [F3411-19], motivated by drafts of European standards, suggest that both Bluetooth versions will be required. If broadcasting Wi-Fi NAN at 5 GHz, it is required to do so concurrently at 2.4 GHz; current discussions in ASTM F38.02 include relaxing this. Wi-Fi Beacons are also under consideration. Future revisions of [F3411-19] may allow other data links.

The selection of Broadcast RID 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 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 31-byte payload limit of the Bluetooth 4.x "Broadcast Frame" transmitted as an "advertisement" on beacon channels. After overheads, this limits the RID message to 25 bytes and the UAS ID string to a maximum length of 20 bytes.

A single Bluetooth 4.x advertisement frame can just barely fit any UAS ID long enough to be sufficiently unique for its purpose.

There is related information, which especially includes, but is not limited to, the UA position and velocity, which must be represented by data elements long enough to provide precision sufficient for their purpose while remaining unambiguous with respect to their reference frame.

In order to enable Observer devices to verify that 1) the claimed UAS ID is indeed owned by the sender and 2) the related information was indeed sent by the owner of that same UAS ID, authentication data elements would typically be lengthy with conventional cryptographic signature schemes. They would be too long to fit in a single frame, even with the latest schemes currently being standardized.

Thus, it is infeasible to bundle information related to the UAS ID and corresponding authentication data elements in a single Bluetooth 4.x frame; yet, somehow all these must be securely bound together.

Messages that cannot be encapsulated in a single frame (thus far, only the Authentication Message) must be segmented into message "pages" (in the terminology of [F3411-19]). Message pages must somehow be correlated as belonging to the same message. Messages

carrying position, velocity and other data must somehow be correlated with the Basic ID Message that carries the UAS ID. This correlation is expected to be done on the basis of Media Access Control (MAC) address. This may be complicated by MAC address randomization. Not all the common devices expected to be used by Observers have APIs that make sender MAC addresses available to user space receiver applications. MAC addresses are easily spoofed. Data elements are not so detached on other media (see Message Pack in the paragraph after next).

[F3411-19] Broadcast RID specifies several message types (see Section 5.4.5 and Table 3 of [F3411-19]). The table below lists these message types. The 4-bit Message Type field in the header can index up to 16 types. Only seven are defined at the time of writing. Only two are mandatory. All others are optional, unless required by a jurisdictional authority, e.g., a CAA. To satisfy both EASA and FAA rules, all types are needed, except Self-ID and Authentication, as the data elements required by the rules are scattered across several message types (along with some data elements not required by the rules).

The Message Pack (type 0xF) is not actually a message but the framed concatenation of at most one message of each type of any subset of the other types, in type index order. Some of the messages that it can encapsulate are mandatory; others are optional. The Message Pack itself is mandatory on data links that can encapsulate it in a single frame (Bluetooth 5.x and Wi-Fi).

Index	Name	Req	Notes
0x0	Basic ID	Mandatory	-
0x1	Location/Vector	Mandatory	-
0x2	Authentication	Optional	paged
0x3	Self-ID	Optional	free text
0x4	System	Optional	-
0x5	Operator ID	Optional	-
0xF	Message Pack	-	BT5 and Wi-Fi

Table 1: Message Types Defined in [F3411-19]

[F3411-19] Broadcast RID specifies very few quantitative performance requirements: static information must be transmitted at least once per three seconds, and dynamic information (the Location/Vector Message) must be transmitted at least once per second and be no older than one second when sent. [FRUR] requires all information be sent at least once per second.

[F3411-19] Broadcast RID transmits all information as cleartext

(ASCII or binary), so static IDs enable trivial correlation of patterns of use, which is unacceptable in many applications, e.g., package delivery routes of competitors.

Any UA can assert any ID using the [F3411-19] required Basic ID Message, which lacks any provisions for verification. The Location/Vector Message likewise lacks provisions for verification and does not contain the ID, so it must be correlated somehow with a Basic ID Message: the developers of [F3411-19] have suggested using the MAC addresses on the Broadcast RID data link, 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 (e.g., X.509). Fetching certificates via the Internet is not always possible (e.g., Observers working in remote areas, such as national forests), so devising a scheme whereby certificates can be transported over Broadcast RID is necessary. 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). Without DRIP extensions to [F3411-19], 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.

At the time of writing, the proposed revision of [F3411-19] defines a new Authentication Type 5 ("Specific Authentication Method (SAM)") to enable SDOs other than ASTM to define authentication payload formats. The first byte of the payload is the SAM Type, used to demultiplex such variant formats. All formats (aside from those for private experimental use) must be registered with ICAO, which assigns the SAM Type. Any Authentication Message payload that is to be sent in exactly the same form over all currently specified Broadcast RID media is limited by lower-layer constraints to a total length of 201 bytes. For Authentication Type 5, which is expected to be used by DRIP, the SAM Type byte consumes the first of these, limiting DRIP authentication payload formats to a maximum of 200 bytes.

3.3. USS in UTM and RID

UAS RID and UTM are complementary; Network RID is a UTM service. The backbone of the UTM system is comprised of multiple USS: one or several per jurisdiction with some being limited to a single jurisdiction while others span multiple jurisdictions. USS also serve as the principal, or perhaps the sole, interface for operators and UAS into the UTM environment. Each operator subscribes to at least one USS. Each UAS is registered by its operator in at least one USS. Each operational intent is submitted to one USS; if approved, that UAS and operator can commence that operation. During the operation, status and location of that UAS must be reported to that USS, which, in turn, provides information as needed about that operator, UAS, and operation into the UTM system and to Observers via Network RID.

USS provide services not limited to Network RID; indeed, the primary USS function is deconfliction of airspace usage between different UAS (and their operators). It will occasionally deconflict UAS from non-UAS operations, such as manned aircraft and rocket launch. Most deconfliction involving a given operation is hoped to be completed prior to commencing that operation; this is called "strategic deconfliction". If that fails, "tactical deconfliction" comes into play; AirBorne DAA (ABDAA) may not involve USS, but Ground-Based DAA (GBDAA) likely will. Dynamic constraints, formerly called "UAS Volume Restrictions (UVRs)", can be necessitated by circumstances such as local emergencies and extreme weather, specified by authorities on the ground, and propagated in UTM.

No role for USS in Broadcast RID is currently specified by regulators or by [F3411-19]. However, USS are likely to serve as registries (or perhaps registrars) for UAS (and perhaps operators); if so, USS will have a role in all forms of RID. Supplemental Data Service Providers (SDSPs) are also likely to find roles, not only in UTM as such but also in enhancing UAS RID and related services. RID services are used in concert with USS, SDSP, or other UTM entities (if and as needed and available). Narrowly defined, RID services provide regulator-specified identification information; more broadly defined, RID services may leverage identification to facilitate related services or functions, likely beginning with V2X.

3.4. DRIP Focus

In addition to the gaps described above, there is a fundamental gap in almost all current or proposed regulations and technical standards for UAS RID. As noted above, ID is not an end in itself, but a means. Protocols specified in [F3411-19] etc. provide limited information potentially enabling (but no technical means 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 location to look for the Remote Pilot; this is slow, at best, and may not be feasible. What if the pilot is on the opposite rim of a canyon, or there are multiple UAS operators to contact whose GCS all lie in different directions from the Observer? An Observer with Internet connectivity and access privileges could look up operator PII in a registry and then call a phone number in hopes that someone who can immediately influence the UAS operation will answer promptly during that operation; this is unreliable, at best, and may not be prudent. Should pilots be encouraged to answer phone calls while flying? Internet technologies can do much better than this.

Thus, to achieve widespread adoption of a RID system supporting safe and secure operation of UAS, protocols must do the following (despite the intrinsic tension among these objectives):

* preserve operator privacy,

* enable strong authentication, and

* enable the immediate use of information by authorized parties.

Just as [F3411-19] is expected to be approved by regulators as a basic means of compliance with UAS RID regulations, DRIP is likewise expected to be approved to address further issues, starting with the creation and registration of Session IDs.

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 a UAS is registered for RID, 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 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.

The foregoing considerations, beyond those addressed by baseline UAS RID standards such as [F3411-19], imply the requirements for DRIP detailed in Section 4.

4. Requirements

The following requirements apply to DRIP as a set of related protocols, various subsets of which, in conjunction with other IETF and external technical standards, may suffice to comply with the regulations in any given jurisdiction or meet any given user need. It is not intended that each and every protocol of the DRIP set, alone, satisfy each and every requirement. To satisfy these requirements, Internet connectivity is required some of the time (e.g., to support DRIP Entity Identifier creation/registration) but not all of the time (e.g., authentication of an asserted DRIP Entity Identifier can be achieved by a fully working and provisioned Observer device even when that device is off-line so is required at all times).

4.1. General

4.1.1. Normative Requirements

GEN-1 Provable Ownership: DRIP MUST enable verification that the asserted entity (typically UAS) ID is that of the actual current sender (i.e., the Entity ID in the DRIP authenticated message set is not a replay attack or other spoof), even on an Observer device lacking Internet connectivity at the time of observation.

GEN-2 Provable Binding: DRIP MUST enable the cryptographic binding of all other [F3411-19] messages from the same actual

current sender to the UAS ID asserted in the Basic ID Message.

GEN-3 Provable Registration: DRIP MUST enable cryptographically secure verification that the UAS ID is in a registry and identification of that registry, even on an Observer device lacking Internet connectivity at the time of observation; 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 application-layer gateways from Broadcast RID to Network RID to stamp messages with precise date/time received and receiver location, then relay them to a network service (e.g., SDSP or distributed ledger) whenever the gateway has Internet connectivity.

GEN-6 Contact: DRIP MUST enable dynamically establishing, with AAA, per policy, strongly mutually authenticated, end-to-end strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including at least the (1) pilot (Remote Pilot or Pilot In Command), (2) the USS (if any) under which the operation is being conducted, and (3) registries in which data on the UA and pilot are held. This requirement applies whenever each party to such desired communications has a currently usable means of resolving the other party's DRIP Entity Identifier to a locator (IP address) and currently usable bidirectional IP (not necessarily Internet) connectivity with the other party.

GEN-7 QoS: DRIP MUST enable policy-based specification of performance and reliability parameters.

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 Registries, SDSP, and potentially others as RID and UTM evolve).

GEN-9 Multihoming: DRIP MUST support multihoming of UA and GCS, for make-before-break smooth handoff and resiliency against path or 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 airspace volumes.

GEN-11 Management: DRIP SHOULD support monitoring of the health and coverage of Broadcast and Network RID services.

4.1.2. Rationale

Requirements imposed either by regulation or by [F3411-19] are not reiterated in this document, but they drive many of the numbered requirements listed here. The regulatory performance requirement in [FRUR] currently would be satisfied by ensuring information refresh rates of at least 1 Hertz, with latencies no greater than 1 second, at least 80% of the time, but these numbers may vary between jurisdictions and over time. Instead, the DRIP QoS requirement is that parameters such as performance and reliability be specifiable by user policy, which does not imply satisfiable in all cases but does imply (especially together with the Management requirement) that when specifications are not met, appropriate parties are notified.

The Provable Ownership requirement addresses the possibility that the actual sender is not the claimed sender (i.e., is a spoofer). DRIP could meet this requirement by, for example, verifying an asymmetric cryptographic signature using a sender-provided public key from which the asserted UAS ID can be at least partially derived. The Provable Binding requirement addresses the problem with MAC address correlation [F3411-19] noted in Section 3.2. The Provable Registration requirement may impose burdens not only on the UAS sender and the Observer's receiver, but also on the registry; yet, it cannot depend upon the Observer being able to contact the registry at the time of observing the UA. The Readability requirement pertains to the structure and format of information at endpoints rather than its encoding in transit, so it may involve machine-assisted format conversions (e.g., from binary encodings) and/or decryption (see Section 4.3).

The Gateway requirement is in pursuit of three objectives: (1) 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; (2) defend against replay attacks; and (3) support optional SDSP services such as multilateration, to complement UAS position self-reports with independent measurements. This is the only instance in which DRIP transports [F3411-19] messages; most of DRIP pertains to the authentication of such messages and identifiers carried in them.

The Contact requirement allows any party that learns a UAS ID (that is a DRIP Entity Identifier rather than another ID Type) to request establishment of a communications session with the corresponding UAS RID sender and certain entities associated with that UAS, but AAA and policy restrictions, inter alia on resolving the identifier to any locators (typically IP addresses), should prevent unauthorized parties from distracting or harassing pilots. Thus, some but not all Observers of UA, receivers of Broadcast RID, clients of Network RID, and other parties can become successfully initiating endpoints for these sessions.

The QoS requirement is only that performance and reliability parameters can be _specified_ by policy, not that any such specifications must be guaranteed to be met; any failure to meet such would be reported under the Management requirement. Examples of such parameters are the maximum time interval at which messages carrying

required data elements may be transmitted, the maximum tolerable rate of loss of such messages, and the maximum tolerable latency between a dynamic data element (e.g., GNSS position of UA) being provided to the DRIP sender and that element being delivered by the DRIP receiver to an application.

The Mobility requirement refers to rapid geographic mobility of nodes, changes of their points of attachment to networks, and changes to their IP addresses; it is not limited to micro-mobility within a small geographic area or single Internet access provider.

4.2. Identifier

4.2.1. Normative Requirements

ID-1 Length: The DRIP Entity Identifier MUST NOT be longer than 19 bytes, to fit in the Specific Session ID subfield of the UAS ID field of the Basic ID Message of the proposed revision of [F3411-19] (at the time of writing).

ID-2 Registry ID: The DRIP identifier MUST be sufficient to identify a registry in which the entity identified therewith is listed.

ID-3 Entity ID: The DRIP identifier MUST be sufficient to enable lookups of other data associated with the entity identified therewith in that registry.

ID-4 Uniqueness: The DRIP identifier MUST be unique within the applicable global identifier space from when it is first registered therein until it is explicitly deregistered therefrom (due to, e.g., expiration after a specified lifetime, revocation by the registry, or surrender by the operator).

ID-5 Non-spoofability: The DRIP identifier MUST NOT be spoofable within the context of a minimal Remote ID broadcast message set (to be specified within DRIP to be sufficient collectively to prove sender ownership of the claimed identifier).

ID-6 Unlinkability: The DRIP identifier MUST NOT facilitate adversarial correlation over multiple operations. If this is accomplished by limiting each identifier to a single use or brief period of usage, the DRIP identifier MUST support well-defined, scalable, timely registration methods.

4.2.2. Rationale

The DRIP identifier can refer to various entities. In the primary initial use case, the entity to be identified is the UA. Entities to be identified in other likely use cases include, but are not limited to, the operator, USS, and Observer. In all cases, the entity identified must own the identifier (i.e., have the exclusive capability to use the identifier, such that receivers can verify the entity's ownership of it).

The DRIP identifier can be used at various layers. In Broadcast RID, it would be used by the application running directly over the data link. In Network RID, it would be used by the application running over HTTPS (not required by DRIP but generally used by Network RID implementations) and possibly other protocols. In RID-initiated V2X applications such as DAA and C2, it could be used between the network and transport layers (e.g., with the Host Identity Protocol (HIP) [RFC9063] [RFC7401]) or between the transport and application layers (e.g., with DTLS [RFC6347]).

Registry ID (which registry the entity is in) and Entity ID (which entity it is, within that registry) 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, registry, or some collaboration among them is unspecified; however, there must be agreement on the UAS ID among these entities. Management of DRIP identifiers is the primary function of their registration hierarchies, from the root (presumably IANA), through sector-specific and regional authorities (presumably ICAO and CAAs), to the identified entities themselves.

While Uniqueness might be considered an implicit requirement for any identifier, here the point of the explicit requirement is not just that it should be unique, but also where and when it should be unique: global scope within a specified space, from registration to deregistration.

While Non-spoofability imposes requirements for and on a DRIP authentication protocol, it also imposes requirements on the properties of the identifier itself. An example of how the nature of the identifier can support non-spoofability is embedding a hash of both the Registry ID and a public key of the entity in the entity identifier, thus making it self-authenticating any time the entity's corresponding private key is used to sign a message.

While Unlinkability is a privacy desideratum (see Section 4.3), it imposes requirements on the DRIP identifier itself, as distinct from other currently permitted choices for the UAS ID (including primarily the static serial number of the UA or RID module).

4.3. Privacy

4.3.1. Normative Requirements

PRIV-1 Confidential Handling: DRIP MUST enable confidential handling of private information (i.e., any and all information that neither the cognizant authority nor the information owner has designated 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 in any situation where it is unlikely that local Observers authorized to access the plaintext will be able to decrypt it or obtain it from a service able to decrypt it. DRIP MUST NOT encrypt data when/where doing so would conflict with applicable regulations or CAA policies/procedures, i.e., DRIP MUST support configurable disabling of encryption.

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

PRIV-4 Public/Private Designation: DRIP SHOULD facilitate designation, by cognizant authorities and information owners, of which information is public and which is private. By default, all information required to be transmitted via Broadcast RID, even when actually sent via Network RID or stored in registries, is assumed to be public; all other information held in registries for lookup using the UAS ID is assumed to be private.

PRIV-5 Pseudonymous Rendezvous: DRIP MAY enable mutual discovery of and communications among participating UAS operators whose UA are in 4-D proximity, using the UAS ID without revealing pilot/operator identity or physical location.

4.3.2. Rationale

Most data to be sent via Broadcast RID or Network RID is public; thus, the Encrypted Transport requirement for private data is selective, e.g., for the entire payload of the Operator ID Message, but only the pilot/GCS location fields of the System Message. Safety critical data includes at least the UA location. Other data also may be deemed safety critical, e.g., in some jurisdictions the pilot/GCS location is implied to be safety critical.

UAS have several potential means of assessing the likelihood that local Observers authorized to access the plaintext will be able to decrypt it or obtain it from a service able to decrypt it. If the UAS is not participating in UTM, an Observer would have no means of obtaining a decryption key or decryption services from a cognizant USS. If the UAS is participating in UTM but has lost connectivity with its USS, then an Observer within visual LOS of the UA is also unlikely to be able to communicate with that USS (whether due to the USS being offline or the UAS and Observer being in an area with poor Internet connectivity). Either of these conditions (UTM non-participation or USS unreachability) would be known to the UAS.

In some jurisdictions, the configurable enabling and disabling of encryption may need to be outside the control of the operator. [FRUR] mandates that manufacturers design RID equipment with some degree of tamper resistance; the preamble of [FRUR] and other FAA

commentary suggest this is to reduce the likelihood that an operator, intentionally or unintentionally, might alter the values of the required data elements or disable their transmission in the required manner (e.g., as cleartext).

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

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

4.4. Registries

4.4.1. Normative Requirements

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 or role 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, according to applicable policy, enforce AAA, including restriction of access to this information based on identity or role 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 U-space/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 AAA MUST be specifiable by policies; the definitive copies of those policies must be accessible in registries; administration of those policies and all DRIP registries must be protected by AAA.

4.4.2. Rationale

Registries are fundamental to RID. Only very limited information can be transmitted via Broadcast RID, but extended information is sometimes needed. The most essential element of information sent is the UAS ID itself, the unique key for lookup of extended information

in registries. The regulatory requirements for the registry information models for UAS and their operators for RID and, more broadly, for U-space/UTM needs are in flux. Thus, beyond designating the UAS ID as that unique key, the registry information model is not specified in this document. While it is expected that registry functions will be integrated with USS, who will provide them is expected to vary between jurisdictions and has not yet been determined in most jurisdictions. However this evolves, the essential registry functions, starting with management of identifiers, are expected to remain the same, so those are specified herein.

While most data to be sent via Broadcast or Network RID is public, much of the extended information in registries will be private. Thus, AAA for registries is essential, not just to ensure that access is granted only to strongly authenticated, duly authorized parties, but also to support subsequent attribution of any leaks, audit of who accessed information when and for what purpose, etc. Specific AAA requirements will vary by jurisdictional regulation, provider philosophy, customer demand, etc., so they are left to specification in policies. Such policies should be human readable to facilitate analysis and discussion, be machine readable to enable automated enforcement, and use a language amenable to both, e.g., eXtensible Access Control Markup Language (XACML).

The intent of the negative and positive access control requirements on registries is to ensure that no member of the public would be hindered from accessing public information, while only duly authorized parties would be enabled to access private information. Mitigation of denial-of-service attacks and refusal to allow database mass scraping would be based on those behaviors, not on identity or role of the party submitting the query per se; however, information on the identity of the party submitting the query might be gathered on such misbehavior by security systems protecting DRIP implementations.

"Internet direct contact information" means a locator (e.g., IP address), or identifier (e.g., FQDN) that can be resolved to a locator, which enables initiation of an end-to-end communication session using a well-known protocol (e.g., SIP).

5. IANA Considerations

This document has no IANA actions.

6. Security Considerations

DRIP is all about safety and security, so content pertaining to such is not limited to this section. This document does not define any protocols, so security considerations of such are speculative. Potential vulnerabilities of DRIP solutions to these requirements 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 by on-path attacker of (i.e., man-in-the-middle attacks on) registration messages

* UA impersonation through private key extraction, improper key sharing, or carriage of a small (presumably harmless) UA, i.e., as a "false flag", by a larger (malicious) UA

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

* message integrity

* non-repudiation

* defense against replay attacks

* defense against spoofing

One approach to so doing involves verifiably binding the DRIP identifier to a public key. Providing these security features, whether via this approach or another, is likely to be especially challenging for Observers without Internet connectivity at the time of observation. For example, checking the signature of a registry on a public key certificate received via Broadcast RID in a remote area presumably would require that the registry's public key had been previously installed on the Observer's device, yet there may be many registries and the Observer's device may be storage constrained, and new registries may come on-line subsequent to installation of DRIP software on the Observer's device. See also Figure 1 and the associated explanatory text, especially the second paragraph after the figure. Thus, there may be caveats on the extent to which requirements can be satisfied in such cases, yet strenuous effort should be made to satisfy them, as such cases are important, e.g., firefighting in a national forest. Each numbered requirement a priori expected to suffer from such limitations (General requirements for Gateway and Contact functionality) contains language stating when it applies.

7. Privacy and Transparency Considerations

Privacy and transparency are important for legal reasons including regulatory consistency. [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.

Transparency (where essential to security or safety) and privacy 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, it is recommended that all DRIP work give due regard to [RFC6973] and, more broadly, to [RFC8280].

However, privacy and transparency are often conflicting goals, demanding careful attention to their balance.

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).

How properly authorized parties are authorized, authenticated, etc. are questions that extend beyond the scope of DRIP, but DRIP may be able to provide support for such processes. Classification of information as public or private must be made explicit and reflected with markings, design, etc. Classifying the information will be addressed primarily in external standards; in this document, it will be regarded as a matter for CAA, registry, and operator policies, for which enforcement mechanisms will be defined within the scope of the DRIP WG and offered. Details of the protection mechanisms will be provided in other DRIP documents. Mitigation of adversarial correlation will also be addressed.

8. References

8.1. Normative References

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", ASTM F3411-19, DOI 10.1520/F3411-19, February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[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

[Amended] European Parliament and Council, "Commission Delegated

Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new unmanned aircraft systems classes", April 2020, <https://eur-lex.europa.eu/eli/reg_del/2020/1058/oj>.

[ASDRI] ASD-STAN, "Introduction to the European UAS Digital Remote ID Technical Standard", January 2021, <https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf>.

[ASDSTAN4709-002] ASD-STAN, "Aerospace series - Unmanned Aircraft Systems - Part 002: Direct Remote Identification", ASD-STAN prEN 4709-002 P1, October 2021, <https://asd-stan.org/downloads/asd-stan-pren-4709-002-p1/>.

[CPDLC] Gurtov, A., Polishchuk, T., and M. Wernberg, "Controller-Pilot Data Link Communication Security", Sensors 18, no. 5: 1636, DOI 10.3390/s18051636, 2018, <https://www.mdpi.com/1424-8220/18/5/1636>.

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", ANSI/CTA 2063-A, September 2019, <https://shop.cta.tech/products/small-unmanned-aerial-systems-serial-numbers>.

[Delegated] European Parliament and Council, "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, <https://eur-lex.europa.eu/eli/reg_del/2019/945/oj>.

[DRIP-ARCH] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., Ed., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-arch-20, 28 January 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-arch-20>.

[ENISACSIRT] European Union Agency for Cybersecurity (ENISA), "Actionable information for Security Incident Response", November 2014, <https://www.enisa.europa.eu/topics/csirt-cert-services/reactive-services/copy_of_actionable-information/actionable-information>.

[EU2018] European Parliament and Council, "2015/0277 (COD) PE-CONS 2/18", June 2018, <https://www.consilium.europa.eu/media/35805/easa-regulation-june-2018.pdf>.

[FAACONOPS] FAA Office of NextGen, "UTM Concept of Operations v2.0",

March 2020, <https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf>.

[FR24] Flightradar24, "About Flightradar24", <https://www.flightradar24.com/about>.

[FRUR] Federal Aviation Administration (FAA), "Remote Identification of Unmanned Aircraft", January 2021, <https://www.federalregister.gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft>.

[GDPR] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", April 2016, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

[ICAOATM] International Civil Aviation Organization, "Procedures for Air Navigation Services: Air Traffic Management", Doc 4444, November 2016, <https://store.icao.int/en/procedures-for-air-navigation-services-air-traffic-management-doc-4444>.

[ICAODEFS] International Civil Aviation Organization, "Defined terms from the Annexes to the Chicago Convention and ICAO guidance material", July 2017, <https://www.icao.int/safety/cargosafety/Documents/Draft%20Glossary%20of%20terms.docx>.

[ICAOUAS] International Civil Aviation Organization, "Unmanned Aircraft Systems", Circular 328, 2011, <https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf>.

[ICAOUTM] International Civil Aviation Organization, "Unmanned Aircraft Systems Traffic Management (UTM) - A Common Framework with Core Principles for Global Harmonization, Edition 3", October 2020, <https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf>.

[Implementing] European Parliament and Council, "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft", May 2019, <https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj>.

[InitialView] SESAR Joint Undertaking, "Initial view on Principles for the U-space architecture", July 2019, <https://www.sesarju.eu/sites/default/files/documents/u-space/SESAR%20principles%20for%20U-

space%20architecture.pdf>.

[LDACS] Maeurer, N., Ed., Graeupl, T., Ed., and C. Schmitt, Ed., "L-band Digital Aeronautical Communications System (LDACS)", Work in Progress, Internet-Draft, draft-ietf-raw-ldacs-09, 22 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-09>.

[NPRM] United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019, <https://www.federalregister.gov/documents/2019/12/31/2019-28100/remote-identification-of-unmanned-aircraft-systems>.

[OpenDroneID] "The Open Drone ID specification", commit c4c8bb8, March 2020, <https://github.com/opendroneid/specs>.

[OpenSky] OpenSky Network, "About the OpenSky Network", <https://opensky-network.org/about/about-us>.

[Opinion1] European Union Aviation Safety Agency (EASA), "High-level regulatory framework for the U-space", Opinion No 01/2020, March 2020, <https://www.easa.europa.eu/document-library/opinions/opinion-012020>.

[Part107] Code of Federal Regulations, "Part 107 - SMALL UNMANNED AIRCRAFT SYSTEMS", June 2016, <https://www.ecfr.gov/cgi-bin/text-idx?node=pt14.2.107>.

[Recommendations] FAA UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC), "UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC): ARC Recommendations Final Report", September 2017, <https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf>.

[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>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[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>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[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>.

[RFC9063] Moskowitz, R., Ed. and M. Komu, "Host Identity Protocol Architecture", RFC 9063, DOI 10.17487/RFC9063, July 2021, <https://www.rfc-editor.org/info/rfc9063>.

[Roadmap] ANSI Unmanned Aircraft Systems Standardization Collaborative (UASSC), "Standardization Roadmap for Unmanned Aircraft Systems", Working Draft, Version 2.0, April 2020, <https://share.ansi.org/Shared Documents/Standards Activities/UASSC/UASSC_20-001_WORKING_DRAFT_ANSI_UASSC_Roadmap_v2.pdf>.

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

[WG105] EUROCAE, "Minimum Operational Performance Standards (MOPS) for Unmanned Aircraft System (UAS) Electronic Identification", WG-105 SG-32 draft ED-282, June 2020.

[WiFiNAN] Wi-Fi Alliance, "Wi-Fi Aware", October 2020, <https://www.wi-fi.org/discover-wi-fi/wi-fi-aware>.

Appendix A. 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 ASTM's "Standard Specification for Remote ID and Tracking" [F3411-19]. Other organizations (for example, in the EU) do not necessarily follow the same architecture.

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 plaintext. Community networks such as OpenSky [OpenSky] and Flightradar24 [FR24] 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-octal 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, that 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 plaintext 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.

The Mode S transponders used in all TCAS and most "ADS-B Out" installations are assigned an ICAO 24-bit "address" (arguably really an identifier rather than a locator) that is associated with the aircraft as part of its registration. In the US alone, well over 2^20 UAS are already flying; thus, a 24-bit space likely would be rapidly exhausted if used for UAS (other than large UAS flying in controlled airspace, especially internationally, under rules other than those governing small UAS at low altitudes).

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 (e.g., WiMAX / IEEE 802.16, 5G) or sensor networks (e.g., 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 [LDACS]. LDACS 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 awareness of global airspace use.

Acknowledgments

The work of the FAA's UAS Identification and Tracking Aviation Rulemaking Committee (ARC) is the foundation of later ASTM [F3411-19] and IETF DRIP efforts. The work of Gabriel Cox, Intel Corp., and their Open Drone ID collaborators opened UAS RID to a wider community. 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 extensively reviewed or otherwise contributed to this document include Amelia Andersdotter, Carsten Bormann, Toerless Eckert, Susan Hares, Mika Jarvenpaa, Alexandre Petrescu, Saulo Da Silva, and Shuai Zhao. Thanks to Linda Dunbar for the SECDIR review, Nagendra Nainar for the OPSDIR review, and Suresh Krishnan for the Gen-ART review. Thanks to IESG members Roman Danyliw, Erik Kline, Murray Kucherawy, and Robert Wilton for helpful and positive comments. Thanks to chairs Daniel Migault and Mohamed Boucadair for direction of our team of authors and editor, some of whom are newcomers to writing IETF documents. Thanks especially to Internet Area Director Éric Vyncke for guidance and support.

This work was partly supported by the EU project AiRMOUR (enabling sustainable air mobility in urban contexts via emergency and medical services) under grant agreement no. 101006601.

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