DRIP S. Card, Ed.
Internet-Draft A. Wiethuechter
Intended status: Informational AX Enterprize
Expires: 5 May 2021 R. Moskowitz
HTT Consulting
A. Gurtov
Linköping University
1 November 2020

Drone Remote Identification Protocol (DRIP) Requirements
draft-ietf-drip-reqs-06

Abstract

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

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

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

Status of This Memo

Commenté [BMT1]: Please update to « Requirements »

Copyright Notice

Table of Contents

1. Introduction ~~(Informative)~~

Commenté [BMT2]: Why this is mentioned here?

1.1. Motivation

Many considerations (especially safety and security) necessitate
Unmanned Aircraft Systems (UAS) Remote Identification and tracking
(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, for
multicopters, of advanced flight stability algorithms, enabling even
inexperienced pilots to take off, fly to a location of interest,
hover, and return to the take-off location or land at a distance.

UAS can be remotely piloted by a human (e.g., with a joystick) or
programmed to proceed from GNSS waypoint to waypoint in a weak form
of autonomy; stronger autonomy is coming. UA are "low observable":
they typically have small radar ~~cross~~ cross-section~~s;~~ . ~~they~~ They make
noise quite
noticeable at short range but difficult to detect at distances they
can quickly close (500 meters in under 17 seconds at 60 knots~~);~~).
~~they~~They
typically fly at low altitudes (e.g., for the small UAS to which RID
applies in the US, under 400 feet AGL~~);~~). ~~they~~ UA are ~~highly~~
maneuverable
so can fly under trees and between buildings.

UA can carry payloads including sensors, cyber and kinetic weapons,
or can be used themselves as weapons by flying them into targets.
They can be flown by clueless, careless, or criminal operators. Thus
the most basic function of UAS RID is "Identification Friend or Foe"
(IFF) to mitigate the significant threat they present. Numerous
other applications can be enabled or facilitated by RID: consider the
importance of identifiers in many Internet protocols and services.
The general scenario is illustrated in Figure 1.

Commenté [BMT3]: Start a new para

Commenté [BMT4]: Expand the acronym

Commenté [BMT5]: Please expand

Commenté [BMT6]: Please consider adding a pointer, if possible.

Commenté [BMT7]: I would cite some few examples.

Commenté [BMT8]: « Scenario » of what?

I would reword as follows: s/scenario/UAS RID usage"

```
                        UA1               UA2
                        x x               x x
                       xxxxx             xxxxx


      General      x                           x     Public
      Public     xxxxx                       xxxxx   Safety
      Observer     x                           x     Observer
                   x                           x
                  x x ---------+  +---------- x x
                 x   x         |  |          x   x
                               |  |
                               +  +
                            xxxxxxxxxx
                           x          x
               +----------+x Internet x+------------+
               |           x          x             |
    UA1      x |            xxxxxxxxxx              | x    UA2
    Pilot  xxxxx               + + +                xxxxx  Pilot
   Operator  x                 | | |                  x  Operator
             x                 | | |                  x
            x x                | | |                 x x
           x   x               | | |                x   x
                               | | |
             +----------+      | | |       +----------+
             |          |------+ | +--------|          |
             | Public   |        |         | Private  |
             | Registry |     +-----+      | Registry |
             |          |     | DNS |      |          |
             +----------+     +-----+      +----------+
```

Figure 1: "General UAS RID Scenario"

Note the absence of any links to/from the UA in Figure 1. This is because UAS RID and other connectivity involving the UA varies as described below.

~~Inherently~~For example, ~~any responsible~~an Observer of UA ~~must~~ will classify them~~,~~ as illustrated notionally in Figure 2. For basic airspace Situational Awareness (SA), an Observer who classifies an UAS: as Taskable, can ask it to do something useful; as Low Concern, can reasonably assume it is not malicious~~,~~ and would cooperate with requests to modify its flight plans for safety concerns that arise; as High Concern or Unidentified, can focus surveillance on it. ~~These classes are not standard, but derive from first principles.~~

Commenté [BMT9]: Many of the components/blocks mentioned in the figure are not introduced in the text. Please consider adding a brief description.

Mis en forme : Surlignage

Mis en forme : Surlignage

```
                              xxxxxxx       +--------------+
                             x       x  No  |              |
                            x   ID?   x+---->| UnidentifiedUNIDENTIFIED |
                             x       x      |              |
                              xxxxxxx       +--------------+
                                 +
                                 | Yes
                                 v
                              xxxxxxx
                             x       x
                  +---------+x  TYPE?  x+----------+
                  |          x       x            |
                  |           xxxxxxx             |
                  |              +                |
                  v              v                v
           +--------------+ +--------------+ +--------------+
           |              | |              | |              |
           |  Taskable~~TASKABLE~~    | | Low Concern~~LOW CONCERN~~  | | High
ConcernHIGH CONCERN |
           |              | |              | |              |
           +--------------+ +--------------+ +--------------+
```

Figure 2: "Notional UAS Classification"

In the context of this document, ~~An~~ an ID (Identifier) is not an end in itself; it exists to enable lookups and provision of services complementing mere identification.

Using UAS RID to facilitate vehicular (V2X) communications and applications such as Detect And Avoid (DAA), which would impose tighter latency bounds than RID itself, is an obvious possibility, explicitly contemplated in the United States (US) Federal Aviation Administration (FAA) Notice of Proposed Rule Making [NPRM]. However, applications of RID beyond RID itself, including DAA, have been declared out of scope in ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041 (source of the widely cited [F3411-19]), based on a distinction between RID as a security standard vs DAA as a safety application. Although dynamic establishment of secure communications between the Observer and the UAS pilot seems to have been contemplated by the FAA UAS ID and Tracking Aviation Rulemaking Committee (ARC) in their [Recommendations], it is not addressed in any of the subsequent proposed regulations or technical specifications.

[Opinion1] and [WG105] cite the Direct Remote Identification previously required and specified, explicitly stating that whereas Direct RID is primarily for security purposes, "Electronic Identification" (or the "Network Identification Service" in the context of U-space) is primarily for safety purposes (e.g., air traffic management, especially hazards deconfliction) and also is

Commenté [BMT10]: To align with the description text.

Commenté [BMT11]: I expect that we will have comments whether this is informative or normative. It seems that we are more close to the normative side vs. informative?

Please double check all the citations of F3411-19 with that in mind and whether that is still aligned with citing the doc as "informative".

Commenté [BMT12]: Consider adding a pointer.

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 one-way to Observers, they will use V2V to other UAS (also likely to and/or from some manned aircraft). These reflect the broad scope of the EU U-space concept, as being developed in the Single European Sky ATM Research (SESAR) Joint Undertaking, whose U-space architectural principles are outlined in [InitialView].

Security oriented UAS RID essentially has two goals: enable the general public to obtain and record an opaque ID for any observed UA, which they can then report to authorities; enable authorities, from such an ID, to look up information about the UAS and its operator. Safety oriented UAS RID has stronger requirements. Aviation community Standards Development Organizations (SDOs) set a higher bar for safety than for security, especially with respect to reliability.

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 all information in UAS RID is operator self-reports. Reports may be initiated by the remote pilot at the Ground Control Station (GCS) console, by a software process on the GCS, or by a process on the UA. Data in the reports may come from the UA (e.g., an on-board GNSS receiver), the GCS (e.g., dead reckoning UA location based on takeoff location and piloting commands given since takeoff), and/or sensors available to the operator (e.g., radar or cameras). Whether information comes proximately from the operator, or from automated systems configured by the operator, there are possibilities not only of unintentional error in, but also of intentional falsification of, this data.

Minimal specified information must be made available to the public~~;~~. ~~access~~ Access to other data, e.g., UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized per policy. The balance between privacy and transparency remains a subject for public debate and regulatory action~~;~~. DRIP can only offer tools to expand the achievable trade space and enable trade-offs within that space. [F3411-19], the basis for most current (2020) 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~~,~~ ~~is~~ are unspecified therein.

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

Commenté [BMT13]: We need to be prepared to have a definition of what we mean here. It is better to explain this in the text.

Commenté [BMT14]: To be expanded

Wireless data links on the UA are challenging due to low altitude flight amidst structures and foliage over terrain, as well as the severe Cost, Size, Weight and Power (CSWaP) constraints of devices onboard UA. CSWaP is a burden not only on the designers of new UA for production and sale, but also on owners of existing UA that must be retrofit. Radio Controlled (RC) aircraft modelers, "hams" who use licensed amateur radio frequencies to control UAS, drone hobbyists, and others who custom build UAS, all need means of participating in UAS RID, sensitive to both generic CSWaP and application-specific considerations.

To accommodate the most severely constrained cases, all these conspire to motivate system design decisions, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of Observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges.

Commenté [BMT15]: Please split this into more sentence to ease readability.

As RID must often operate with limited bandwidth, short packet payload length limits, and one-way links, 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 string (typically number) itself can be merely an unsubstantiated claim.

Commenté [BMT16]: Do we need this precision at this stage?

Mis en forme : Surlignage

Observer devices being ubiquitous, thus popular targets for malware or other compromise, cannot be generally trusted (although the user of each device is compelled to trust that device, to some extent); a "fair witness" functionality (inspired by [Stranger]) is desirable.

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

1.3. DRIP Scope

DRIP's initial goal is to make RID immediately actionable, in both Internet and local-only connected scenarios (especially emergencies), in severely constrained UAS environments, balancing legitimate (e.g., public safety) authorities' Need To Know trustworthy information with UAS operators' privacy. By "immediately actionable" is meant information of sufficient precision, accuracy, timeliness, etc. for an Observer to use it as the basis for immediate decisive action, whether that be to trigger a defensive counter-UAS system, to attempt to initiate communications with the UAS operator, to accept the presence of the UAS in the airspace where/when observed as not requiring further action, or whatever, with potentially severe consequences of any action or inaction chosen based on that information. For further explanation of the concept of immediate actionability, see [ENISACSIRT]. Note that UAS RID must achieve near universal adoption, but DRIP can add value even if only selectively deployed, as those with jurisdiction over more sensitive airspace volumes may set a higher than generally mandated RID bar for flight in those volumes. Providing timely trustworthy identification data is also prerequisite to identity-oriented networking.

Commenté [BMT17]: I quite agree with this but I think this is a distraction for the main goal of the document. I would delete this sentence.

DRIP ~~(originally Trustworthy Multipurpose Remote Identification, TM-RID)~~ potentially could be applied to verifiably identify other types of registered things reported to be in specified physical locations, but the urgent motivation and clear initial focus is UAS. Existing Internet resources (protocol standards, services, infrastructure, and business models) should be leveraged.

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

Commenté [BMT18]: I suggest to move this text to 1.4.

1.4 Scope

Commenté [BMT19]: We need to describe the scope & objectives of the document: problem space, common terminology, and requirements.

Commenté [BMT20]: We also need to add a pointer to « Discussion and Limitations" to ACK.

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~~ some of the terms listed below are not used in this document.

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

Commenté [BMT21]: Start a new para

In the UAS community, the plural form of acronyms generally is the same as the singular form, e.g., Unmanned Aircraft System (singular) and Unmanned Aircraft Systems (plural) are both represented as UAS. On this and other terminological issues, to encourage comprehension necessary for adoption of DRIP by the intended user community, that community's norms are respected herein, and definitions are quoted in cases where they have been found in that community's documents. Most of the listed terms are from that community (even if specific source documents are not cited); any that are DRIP-specific or invented by the authors of this document are marked "(DRIP)".

Commenté [BMT22]: Start a new para.

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

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

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

Authentication Message
~~[F3411-19] Message Type 2~~. Provides framing for authentication data, only. It is also known as [F3411-19] Message Type 2~~Optional per [F3411-19] but may be required by regulations.~~

Commenté [BMT23]: We need to avoid mixing term definitions vs. requirements.

Basic ID Message
[F3411-19] Message Type 0. Provides UA Type, UAS ID Type and UAS ID, only. ~~Mandatory per [F3411-19].~~

Commenté [BMT24]: We need to avoid mixing term definitions vs. requirements.

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

Commenté [BMT25]: This conflicts with the introduction. Suggest to delete the entry.

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

CAA
Civil Aviation Authority. Two examples are the United States Federal Aviation Administration (FAA) and the 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, 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 it as "t~~T~~he capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action to comply with the applicable rules of flight~~.~~" ~~[ICAOUAS]~~.

Direct RID

Direct Remote Identification. It is "a system that ensures the local broadcast of information about an UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA"~~.~~ [Delegated]. It ~~Corresponds~~corresponds roughly to the Broadcast RID portion of [NPRM] Standard RID.

DSS

Discovery and Synchronization Service. Formerly Inter-USS. 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 deconfliction of planned and Network RID surveillance of active operations~~.~~ [F3411-19].

EUROCAE

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

GBDAA

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

GCS

Ground Control Station. The part of the UAS that the remote pilot uses to exercise C2 over the UA, whether by remotely exercising UA flight controls to fly the UA, by setting GPS waypoints, or otherwise directing its flight.

GNSS

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

GPS

Global Positioning System. A specific GNSS, but in 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 per IATF, dedicated to aviation (but not just aircraft). ~~Currently in design.~~

IATF

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

ICAO

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

LAANC

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

Limited RID

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

Location/Vector Message

[F3411-19] Message Type 1. Provides UA location, altitude, heading, speed and status. ~~Mandatory per [F3411-19].~~

LOS

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

MSL

Mean Sea Level. Relative altitude, above the variously defined mean sea level, typically of an UA (but in [NPRM] also for a GCS), measured in feet or meters. Should be explicitly specified as either barometric (pressure) or geodetic (GNSS).

Net-RID DP

Network RID Display Provider. ~~[F3411-19]~~A 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 [NPRM], not recognized as a distinct entity, but a service provided by USS, including Public Safety USS that may exist primarily for this purpose rather than to manage any subscribed UAS.

Net-RID SP
Network RID Service Provider. ~~[F3411-19]~~A logical entity that collects RID messages from UAS and responds to NetRID-DP queries for information on UAS of which it is aware. Under [NPRM], the USS to which the UAS is subscribed ("Remote ID USS").

Network Identification Service
EU regulatory requirement for Network RID. [Opinion1] and [WG105] Corresponds roughly to the Network RID portion of [NPRM] Standard RID.

Commenté [BMT26]: Not sure why this are cited here.

Observer
An entity (typically but not necessarily an individual human) who has directly or indirectly observed an UA and wishes to know something about it, starting with its ID. An observer typically is on the ground and local (within V-LOS 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~~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. ~~Optional per [F3411-19] but may be required by regulations.~~Also known as [F3411-19] Message Type 5.

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 this context, typically of the UAS Operator, Pilot In Command (PIC) or Remote Pilot, but possibly of an Observer or other party.

Commenté [BMT27]: Which one ?

Remote Pilot
A pilot using a GCS to exercise proximate control of an 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. ~~Noun or adjective, e.g. "RF link."~~

RF-LOS
RF LOS. 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 V-LOS.

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

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. ~~Optional per [F3411-19] but may be required by regulations.~~ Also known as [F3411-19] Message Type 3.

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

SDO
Standards Development Organization such as~~.~~ ASTM, IETF, ~~et al~~etc.

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

Commenté [BMT28]: I'm not sure this is needed in the definition section

Mis en forme : Surlignage

System Message
~~[F3411-19] Message Type 4.~~ Provides general UAS information, including remote pilot location, multiple UA group operational area, etc. ~~Optional per [F3411-19] but may be required by regulations.~~It is also known as [F3411-19] Message Type 4.

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

Mis en forme : Surlignage

UAS ID Type
UAS Identifier type index. 4 bits, see Section 3, Paragraph 5 for currently defined values 0-3. [F3411-19]

Commenté [BMT29]: This is clearly arguing for listing the ref as normative.

UAS RID
UAS Remote Identification and tracking. Refers to s ~~System~~ system to enable arbitrary Observers to identify UA during flight.

UAS RID Verifier Service
System component designed to handle the authentication requirements of RID by offloading verification to a web hosted service. ~~[F3411-19]~~

USS

UAS Service Supplier. "A USS is an entity that assists UAS Operators with meeting UTM operational requirements that enable safe and efficient use of airspace" and "... provide services to support the UAS community, to connect Operators and other entities to enable information flow across the USS Network, and to promote shared situational awareness among UTM participants" as per [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, per FAA, a "traffic management" ecosystem for "uncontrolled" low altitude UAS operations, separate from, but complementary to, the FAA's ATC system for "controlled" operations of manned aircraft.

V2V

Vehicle-to-Vehicle. Originally communications between automobiles, now extended to apply to communications between vehicles generally. Often, together with Vehicle-to-Infrastructure (V2I) etc., generalized to V2X.

V-LOS

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

3. UAS RID Problem Space

Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The US FAA has described the key role that UAS RID plays in UAS Traffic Management (UTM) in [NPRM] and [FAACONOPS] (especially Section 2.6 of the latter). CAAs currently (2020) promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM developed a widely cited Standard Specification for Remote ID and Tracking [F3411-19] (early drafts are freely available as [OpenDroneID] specifications). It defines two means of UAS RID:

Commenté [BMT30]: I would cite this earlier in the document.

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~~WLAN (without IP or any other protocols between the data link and application layer), to be received in real time by local Observers.

Commenté [BMT31]: Wi-Fi is a trademark. Please use WLAN instead.

UAS using both means must send the same UAS RID application layer information via each as per [F3411-19] and [NPRM]. 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).

Mis en forme : Surlignage

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 for UAS registry information lookup using the directly locally received UAS Identifier (UAS ID) as a key. Broadcast RID does not assume IP connectivity of UAS; messages are encapsulated by the UA without IP, directly in Bluetooth or ~~WiFi~~ WLAN link layer frames.

[F3411-19] specifies three UAS ID types:

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

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

TYPE-3 A UTM system assigned UUID [RFC4122], which can but need not be dynamic.

Per [Delegated], the EU allows only Type 1. Per [NPRM], the US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once as a "Session ID" (for a single UAS flight, which in the context of UTM is called an "operation"). 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. Per [NPRM], the US allows but does not require that operator registration numbers be sent. As yet apparently there are no CAA public proposals to use Type 2.

3.1. Network RID

```
             x x    UA
            xxxxxxx
             |    \
             |     \
             |      \
             |       \  ********************
             |        \*              ------*---+------------+
             |        *\             /       *  | NET_Rid_SP |
             |        * ------------/    +---*--+------------+
             | RF     */                 |   *
             |        /      INTERNET    |   *  +------------+
             |       /*                  +---*--| NET_Rid_DP |
             |      / *                 +----*--+------------+
             +     /   *                |   *
              x   /     ****************|***      x
            xxxxx                       |       xxxxx
              x                         +-------  x
              x                                   x
             x x   Operator's GCS      Observer  x x
            x   x                               x   x
```

Figure 3: "Network RID Information Flow"

Commenté [BMT32]: Not called out in the text.

Only two of the three links UA-GCS, UA-Internet, and GCS-Internet need exist, although all three may exist. There must be some path (direct or indirect) between the GCS and the UA, for the former to exercise C2 over the latter~~;~~ . ~~if~~ 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) information to the GCS. There must be some 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 Net-RID SP).

Commenté [BMT33]: How path is defined here?

Mis en forme : Surlignage

~~Currently, t~~The RID data flow typically originates on the UA and passes through the GCS, or originates on the GCS, rather than comes direct from the UA as in Broadcast RID (below), and makes up to three trips through the Internet, implying use of IP (and other middle layer protocols) on those trips, but not necessarily on an UA-GCS link (if indeed that direct even exists and further the Network RID data flows across it).

Commenté [BMT34]: Please consider splitting this too long sentence.

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~~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 an 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 DP) 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 unspecified (generally presumed to be web browser based) means.

Network RID has several variants. The UA may have persistent onboard Internet connectivity, in which case it can consistently source RID information directly over the Internet. The UA may have intermittent onboard Internet connectivity, in which case the GCS must source RID information whenever the UA itself is offline. The UA may not have Internet connectivity of its own, but have instead some other form of communications to another node that can relay RID information to the Internet~~;~~. ~~this~~ This would typically be the GCS (which to perform its function must know where the UA is, although C2 link outages do occur).

Mis en forme : Surlignage

The UA may have no means of sourcing RID information, in which case the GCS must source it; this is typical under FAA NPRM Limited RID proposed rules, which require providing the location of the GCS (not that of the UA). In the extreme case, this could be the pilot using a web browser/application to designate, to an UAS Service Supplier (USS) or other UTM entity, a time-bounded airspace volume in which an operation will be conducted; this may impede disambiguation of ID if multiple UAS operate in the same or overlapping 4-D volumes.

In most cases in the near term, if the RID information is fed to the Internet directly by the UA or GCS, the first hop data links will be , e.g., cellular Long Term Evolution (LTE) or ~~Wi-Fi~~WLAN, but provided the data link can support at least UDP/IP and ideally also TCP/IP, its type is generally immaterial to the higher layer protocols. An UAS as the ultimate source of Network RID information feeds an USS acting as a Network RID Service Provider (Net-RID SP), which essentially proxies for that and other sources; an observer or other ultimate consumer of Network RID information obtains it from a Network RID Display Provider (Net-RID DP), which aggregates information from multiple Net-RID SPs to offer 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, accessible via typical means such as web APIs/ browsers.

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

Commenté [BMT35]: This has to be assessed.

3.2. Broadcast RID

```
             x x  UA
            xxxxx
             |
             |
             | app messages directly over one-way RF data link
             |
             |
             +
              x
            xxxxx
              x
              x
             x x   Observer's device (e.g. smartphone)
            x   x
```

Figure 4: "Broadcast RID Information Flow"

Commenté [BMT36]: Not cited in the text.

Note the absence of the Internet from this information flow sketch. This is because Broadcast RID is one-way direct transmission of application layer messages over a RF data link (without IP or other middle layer protocols) 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 verifier service and look up information in registries using the UAS ID as the primary unique key.

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

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

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

~~[F3411-19]~~ Broadcast RID specifies several message types [F3411-19]: Basic, Location, Authentication, Self-ID, System, and Operator ID. To satisfy EASA and FAA proposed rules, all types are needed, except Authentication and Self-ID.

~~[F3411-19]~~ Broadcast RID specifies very few quantitative performance Requirements [F3411-19]: static information must be transmitted at least once per 3 seconds; dynamic information (the Location message) must be transmitted at least once per second and be no older than one second when sent. [NPRM] proposes 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, unacceptable in many applications, e.g., package delivery routes of competitors [F3411-19].

Any UA can assert any ID using the [F3411-19] required Basic ID message, which lacks any provisions for verification. The Position/ Vector message likewise lacks provisions for verification, and does not contain the ID, so must be correlated somehow with a Basic ID message: the developers of [F3411-19] have suggested using the MAC addresses 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. The one-way nature of Broadcast RID precludes challenge-response security protocols (e.g., observers sending nonces to UA, to be returned in signed messages). An observer would be seriously challenged to validate the asserted UAS ID or any other information about the UAS or its operator looked up therefrom.

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; some limited to a single jurisdiction, others spanning 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; from this point until the end of 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 by different UAS and other (e.g., manned aircraft, rocket launch) operations. Most deconfliction involving a given operation is hoped to be completed prior to commencing that operation, and is called "strategic deconfliction~~.~~". If that fails, "tactical deconfliction" comes into play~~;~~ . ABDAA may not involve USS, but GBDAA likely will. Also, dynamic constraints (formerly UAS Volume Restrictions~~,~~ (UVR)) can be necessitated by local emergencies, extreme weather, etc., specified by authorities on the ground and propagated in UTM.

No role for USS in Broadcast RID is currently specified by regulators or [F3411-19]. However, USS are likely to serve as registries (or perhaps registrars) for UAS (and perhaps operators~~);~~). ~~if~~ If so, USS will have a role in all forms of RID. Supplemental Data Service Providers (SDSP) are also likely to find roles, not only in UTM as such but also in enhancing UAS RID and related services. Whether USS, SDSP, etc. are involved or not, RID services, narrowly defined, 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. Documents such as [F3411-19]~~ etc.~~ provide very limited choices for an observer to communicate with the pilot, e.g., to request further information on the UAS operation or exit from an airspace volume in an emergency. The System Message provides the location of the pilot/GCS, so an observer could physically go to the asserted location to look for the remote pilot; this is at best slow, and may not be feasible -- what if the pilot is on the opposite rim of a canyon, or there are multiple UAS operators to be contacted 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, then call a phone number in hopes someone who can immediately influence the UAS operation will answer promptly during that operation; this is unreliable. Internet technologies can do much better than this.

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

DRIP will focus on making information obtained via UAS RID immediately usable:

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

2. by enabling verification that an UAS is registered 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.

xx

Commenté [BMT37]: Consider adding a transition text to the requirements.

4. Requirements

4.1. General

GEN-1 Provable Ownership: DRIP MUST enable verification that the UAS ID asserted in the Basic ID message is that of the actual current sender of the message (i.e., the message is not a replay attack or other spoof, authenticating, e.g., by verifying an asymmetric cryptographic signature using a sender provided public key from which the asserted ID can be at least partially derived), even on an observer device lacking Internet connectivity at the time of observation.

Commenté [BMT38]: We need to indicate somewhere in the doc that one or many solutions are needed to achieve DRIP gaols. These solutions are called "DRIP in this section.

GEN-2 Provable Binding: DRIP MUST enable binding 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 verification that the UAS ID is in a registry and identification of which one, even on an observer device lacking Internet connectivity at the time of observation; with UAS ID Type 3, the same sender may have multiple IDs, potentially in different registries, but each ID must clearly indicate in which registry it can be found.

GEN-4 Readability: DRIP MUST enable information (regulation required elements, whether sent via UAS RID or looked up in registries) to be read and utilized by both humans and software.

GEN-5 Gateway: DRIP MUST enable Broadcast RID to Network RID application layer gateways to stamp messages with precise date/time received and receiver location, then relay them to a network service (e.g., SDSP or distributed ledger), to support three objectives: (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).

GEN-6 Finger: DRIP MUST enable dynamically establishing, with AAA, per policy, ~~end ~~end-~~to ~~to-end strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including at least the remote pilot and USS.

GEN-7 QoS: DRIP MUST enable policy based specification of performance and reliability parameters, such as maximum message transmission intervals and delivery latencies.

GEN-8 Mobility: DRIP MUST support physical and logical mobility of UA, GCS, and Observers. DRIP SHOULD support mobility of essentially all participating nodes (UA, GCS, Observers, Net-RID SP, Net-RID DP, Private Registry, and SDSP).

GEN-9 Multihoming: DRIP MUST support multihoming of UA and GCS, for make-before-break smooth handoff and resiliency against path/link failure. DRIP SHOULD support multihoming of essentially all participating nodes.

GEN-10 Multicast: DRIP SHOULD support multicast for efficient and flexible publish-subscribe notifications, e.g., of UAS reporting positions in designated airspace volumes.

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

Requirements imposed either by regulation or [F3411-19] are not reiterated here, but drive many of the numbered requirements listed here. The [NPRM] regulatory QoS requirement 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. So instead the DRIP QoS requirement is that performance, reliability, etc. parameters be user policy specifiable, which does not imply satisfiable in all cases, but (especially together with the management requirement) implies 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). The "provable binding" requirement addresses the MAC address correlation problem of [F3411-19] noted above. 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 may involve machine assisted format conversions, e.g., from binary encodings. The "gateway" requirement is the only instance in which DRIP transports [F3411-19] messages; most of DRIP pertains to the authentication of such messages and the identifier carried within them.

4.2. Identifier

ID-1 Length: The DRIP (UAS) entity (remote) identifier ~~must~~ MUST NOT be ~~no~~ longer than 20 bytes. This is particularly to align with ~~(per~~ [F3411-19] to fit in a Bluetooth 4 advertisement payload~~)~~.

Commenté [BMT39]: The use of parentheses makes it hard to follow the meaning of the requirement. The same comment applies for other requirements. Please reword.

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

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

ID-4 Uniqueness: The DRIP identifier MUST be unique within the global UAS RID identifier space from when it is first registered therein until it is explicitly de-registered therefrom (due to, e.g., expiration after a specified lifetime such as the FAA's proposed 6 months RID data retention period, revocation by the registry, or surrender by the operator).

ID-5 Non-spoofability: The DRIP identifier MUST NOT be ~~non-~~spoofable within the context of Remote ID broadcast messages (some collection of messages provides proof of UA ownership of ID).

Commenté [BMT40]: I'm afraid more elaboration is needed.

ID-6 Unlinkability: A DRIP UAS ID MUST NOT facilitate adversarial correlation over multiple UAS operations~~;~~. ~~this~~ This may be accomplished, e.g., by limiting each identifier to a single use, but if so, the UAS ID MUST support well-defined scalable timely registration methods.

Commenté [BMT41]: We may be challenged whether we can define this more concretely.

The DRIP identifier can be used at various layers~~:~~. ~~in~~ 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 (and possibly other protocols).~~; and~~ ~~in~~ In RID initiated V2X applications such as DAA and C2, it could be used between the network and transport layers ~~(with HIP or DTLS)~~.

Commenté [BMT42]: I don't see the need to mention these.

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 an UAS ID is generated by the operator, GCS, UA, USS or registry, or some collaboration thereamong~~,~~ is unspecified. ~~;~~ ~~however~~However, there must be agreement on the UAS ID among these entities.

4.3. Privacy

PRIV-1 Confidential Handling: DRIP MUST enable confidential handling of private information (i.e., any and all information designated by neither cognizant authority nor the information owner as public, e.g., personal data).

PRIV-2 Encrypted Transport: DRIP MUST enable selective strong encryption of private data in motion in such a manner that only authorized actors can recover it. If transport is via IP, then encryption MUST be end-to-end, at or above the IP layer. DRIP MUST NOT encrypt safety critical data to be transmitted over Broadcast RID in any situation where it is unlikely that local O~~o~~bservers 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. As such, ~~i.e.~~ DRIP MUST support configurable disabling of encryption.

Commenté [BMT43]: Which ends ?

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, which information is public and which private. By default, all information required to be transmitted via Broadcast RID, even when actually sent via Network RID, is assumed to be public; all other information contained 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.

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 requires obfuscation of location to any Network RID subscriber engaging in wide area surveillance, limits data retention periods, etc. in the interests of privacy), 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

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, per 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 MUST enable closing the AAA-policy registry loop by governing AAA per registered policies and administering policies only via AAA.

Commenté [BMT44]: What does this mean ?

Registries are fundamental to RID. Only very limited information can be Broadcast, 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. Beyond designating the UAS ID as that unique key, the registry information model is not specified herein, in part because regulatory requirements for different registries (UAS operators and their UA, each narrowly for UAS RID and broadly for U-space/UTM) and business models for meeting those requirements are in flux. However those may evolve, the essential registry functions remain the same, so are specified herein.

5. IANA Considerations

This document does not make any IANA request.

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 specify any protocol but ~~P~~potential vulnerabilities of DRIP solutions include but are not limited to:

- Sybil attacks.

- Confusion created by many spoofed unsigned messages.

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

- Malicious or malfunctioning registries.

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

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

It may be inferred from the ~~Section 4.1 General~~ general requirements for ~~Provable~~ provable ~~Ownership~~ownership, ~~Provable~~ provable ~~Binding~~ binding, and ~~Provable~~ provable ~~Registration~~registration discussed in Section 4.1, together with the ~~Section 4.2 Identifier~~ 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. ~~E.g.~~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. Thus there may be caveats on the extent to which requirements can be satisfied in such cases, yet strenuous effort should be made to satisfy them, as such cases, e.g.,~~.~~ firefighting in a national forest, are important.

7. Privacy and Transparency Considerations

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

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

DRIP information falls into two classes: that which, to achieve the purpose, must be published openly as cleartext, for the benefit of any Observer (e.g., the basic UAS ID itself); and that which must be protected (e.g., PII of pilots) but made available to properly authorized parties (e.g., public safety personnel who urgently need to contact pilots in emergencies).

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; herein it will be regarded as a matter for CAA, registry and operator policies, for which enforcement mechanisms will be defined within the scope of DRIP WG and offered. Details of the protection mechanisms will be provided in other DRIP documents. Mitigation of adversarial correlation will also be addressed.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

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

8.2. Informative References

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

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

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

[drip-architecture] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", Work in Progress, Internet-Draft, draft-ietf-drip-arch-04, 28 October 2020, <https://tools.ietf.org/html/draft-ietf-drip-arch-04>.

[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>.

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

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

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

[I-D.maeurer-raw-ldacs]
Maeurer, N., Graeupl, T., and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)", Work in Progress, Internet-Draft, draft-maeurer-raw-ldacs-06, 2 October 2020, <https://tools.ietf.org/html/draft-maeurer-raw-ldacs-06>.

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

[ICAOUAS] International Civil Aviation Organization, "Circular 328: Unmanned Aircraft Systems", February 2011.

[ICAOUTM] International Civil Aviation Organization, "Unmanned Aircraft Systems Traffic Management (UTM) - A Common Framework with Core Principles for Global Harmonization, Edition 2", November 2019.

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

[InitialView]
SESAR Joint Undertaking, "Initial view on Principles for the U-space architecture", July 2019.

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

[OpenDroneID]
Intel Corp., "Open Drone ID", March 2019, <https://github.com/opendroneid/specs>.

[Opinion1] European Union Aviation Safety Agency (EASA), "Opinion No 01/2020: High-level regulatory framework for the U-space", March 2020.

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

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

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

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

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

[Roadmap] American National Standards Institute (ANSI) Unmanned Aircraft Systems Standardization Collaborative (UASSC), "Standardization Roadmap for Unmanned Aircraft Systems draft v2.0", April 2020, <https://share.ansi.org/Shared Documents/Standards Activities/UASSC/UASSC_20-001_WORKING_DRAFT_ANSI_UASSC_Roadmap_v2.pdf>.

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

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

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 this standard. Other organizations, for example in EU, do not necessary 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 plain text. Community networks such as OpenSky and Flightradar use this open information through ADS-B to deploy public services of flight tracking. Many researchers also use these data to perform optimization of routes and airport operations. Such ID information should be integrity protected, but not necessarily confidential.

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

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

~~Wi-Fi~~WLAN and Bluetooth are two wireless technologies currently recommended by ASTM specifications due to their widespread use and broadcast nature. However, those have limited range (max 100s of meters) and may not reliably deliver UAS ID at high altitude or distance. Therefore, a study should be made of alternative technologies from the telecom domain (WiMAX~~ ~~/~~ ~~IEEE 802.16, 5G) or sensor networks (Sigfox, LORA). Such transmission technologies can impose additional restrictions on packet sizes and frequency of transmissions, but could provide better energy efficiency and range. In civil aviation, Controller-Pilot Data Link Communications (CPDLC) is used to transmit command and control between the pilots and ATC. It could be considered for UAS as well due to long range and proven use despite its lack of security [cpdlc].

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

Acknowledgments

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM [F3411-19] and IETF DRIP efforts. The work of 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, Mohamed Boucadair, Toerless Eckert, Susan Hares, Mika Jarvenpaa, Daniel Migault, Alexandre Petrescu, Saulo Da Silva and Shuai Zhao.

Authors' Addresses

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

Email: stu.card@axenterprize.com

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

Email: adam.wiethuechter@axenterprize.com

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

Email: rgm@labs.htt-consult.com

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping
Sweden

Email: gurtov@acm.org