Workgroup: TMRID
Internet-Draft: draft-card-tmrid-uas-arch-00
Published: 5 February 2020
Intended Status: Informational
Expires: 8 August 2020
Authors: S. Card A. Wiethuechter R. Moskowitz
AX Enterprize AX Enterprize HTT Consulting

Unmanned Aircraft System Remote Identification Architecture

Abstract

This document defines an architecture for Trustworthy Multipurpose Remote Identification (tm-rid) protocols and services to support Unmanned Aircraft System Remote Identification (UAS RID), including its building blocks and their interfaces, all to be standardized.

Status of This Memo

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

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

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

This Internet-Draft will expire on 8 August 2020.

Copyright Notice

Table of Contents

1. Introduction

Many safety and other considerations dictate that UAS be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published Commision Delegated Regulation 2019/945 and Commission Implementing Regulation 2019/947. The United States (US) Federal Aviation Administration (FAA) has published a Notice of Proposed Rule Making (NPRM). CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

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

[WK65041] specifies 3 UAS ID types. Type 1 is a static, manufacturer assigned, hardware serial number per ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A]. Type 2 is a CAA assigned (presumably static) ID. Type 3 is a UAS Traffic Management (UTM) system assigned UUID [RFC4122], which can but need not be dynamic. The EU allows only Type 1; the US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once. [WK65041] Broadcast RID transmits all information in the clear as plaintext, so Type 1 static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g. package delivery routes of competitors.

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

Minimal specified information must be made available to the public; access to other data, e.g. UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized per policy. [WK65041] specifies only how to get the UAS ID to the observer; how the observer can perform these lookups, and how the registries first can be populated with information, is unspecified.

Although using UAS RID to facilitate related services, such as Detect And Avoid (DAA) and other applications of Vehicle to Vehicle or Vehicle to Infrastructure (V2V, V2I, collectively V2X) communications, is an obvious application (explicitly contemplated in the FAA NPRM), it has been ommitted from [WK65041] (explicitly declared out of scope in the ASTM working group discussions based on a distinction between RID as a security standard vs DAA as a safety application). Although dynamic establishment of secure communications between the observer and the UAS pilot seems to have been contemplated by the FAA Aviation Rulemaking Committee (ARC), it is not addressed in any of the subsequent proposed regulations or technical specifications.

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by observers of already ubiquitous mobile devices (smartphones and tablets). UA onboard RID devices are severely constrained in Size, Weight and Power (SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and observer receive RID capabilities. To accomodate 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. Heavyweight security protocols are infeasible, yet trustworthiness of UAS RID information is essential. Under [WK65041], even the most basic datum, the UAS ID string (typically number) itself can be merely an unsubstantiated claim.

IETF can help by providing expertise as well as mature and evolving standards. Existing Internet resources (business models, infrastructure and protocol standards) should be leveraged. Host Identity Protocol (HIPv2) [RFC7401] and its Domain Name System (DNS) extensions [RFC8005], together with the Registry Data Access Protocl (RDAP) and the Extensible Provisioning Protocol (EPP), can complement emerging external standards for UAS RID. This will facilitate utilization of existing and provision of enhanced network services, and enable verification that UAS RID information is trustworthy (to some extent, even in the absence of Internet connectivity at the receiving node). The natural Internet architecture for UAS RID described herein addresses requirements defined in a companion UAS RID Requirements document.

2. Terms and Definitions

2.1. Requirements Terminology

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

2.2. Definitions

$SWaP
: Cost, Size, Weight and Power.

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

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

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

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

C2
: Command and Control. A set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions. Mainly used in military contexts.

CS-RID
: Crowd Sourced Remote Identification. An optional TM-RID service that gateways Broadcast RID to Network RID, and supports verification of RID positon/velocity claims with independent measurements (e.g. by multilateration), via a SDSP.

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

E2E
: End to End.

GBDAA
: Ground Based DAA.

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

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

GPS

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

HI

Host Identity. The public key portion of an asymmetric keypair from HIP. In this document it is assumed that the HI is based on a EdDSA25519 keypair. This is supported by new crypto defined in [I-D.moskowitz-hip-new-crypto].

HIP

Host Identity Protocol. The origin of HI, HIT, and HHIT, required for TM-RID. Optional full use of HIP enables additional TM-RID functionality.

HHIT

Hierarchical Host Identity Tag. A HIT with extra information not found in a standard HIT. Defined in [I-D.moskowitz-hip-hierarchical-hit].

HIT

Host Identity Tag. A 128 bit handle on the HI. Defined in HIPv2 [RFC7401].

Limited RID

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

LOS

Line Of Sight. An adjectival phrase describing any information transfer that travels in a nearly straight line (e.g. electromagnetic energy, whether in the visual light, RF or other

frequency range) and is subject to blockage. A term to be avoided due to ambiguity, in this context, between RF-LOS and V-LOS.

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

NETDP
UAS RID Display Provider. System component that requests data from one or more NETSP and aggregates them to display to a user application on a device. Often an USS.

NETSP
UAS RID Service Provider. System component that compiles information from various sources (and methods) in its given service area. Usually an USS.

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

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

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

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

SDSP
Supplemental Data Service Provider. Entity that provides data allowed and presumed useful but neither required nor standardized as an option in UTM, such as weather. Here used to enable CS-RID.

Standard RID
Per the FAA NPRM, a mode of operation that must use both Network RID (if Internet connectivity is available at the time in the operating area) and Broadcast RID (always and everywhere), and must provide both pilot/GCS location and UA location. This mode is required for UAS that exceed the allowed envelope (e.g. size,

range) of Limited RID and for all UAS equipped for Standard RID (even if operated within parameters that would otherwise permit Limited RID).

UA
: Unmanned Aircraft. Typically a military or commercial "drone" but can include any and all aircraft that are unmanned.

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

UAS ID
: Unique UAS identifier. Per [WK65041], maximum length of 20 bytes.

UAS ID Type
: Identifier type index. Per [WK65041], 4 bits, values 0-3 already specified.

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

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

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

UTM
: UAS Traffic Management. A "traffic management" ecosystem for "uncontrolled" UAS operations separate from, but complementary to, the FAA's Air Traffic Management (ATM) system for "controlled" operations of manned aircraft.

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

subject to blockage by foliage, structures, terrain or other vehicles, more so than RF-LOS.

3. Entities and their Interfaces

Any tm-rid solutions for UAS RID must fit into the UTM system. This implies interaction with entities including UA, GCS, USS, NETSP, NETDP, Observers, Operators, Pilots In Command, Remote Pilots, etc. The only additional entities introduced by tm-rid are registries, required but not specified by the regulations and [RFC7401], and optionally CS-RID SDSP and Finder nodes.

UAS RID registries hold both public and private information. The public information is primarily pointers to the repositories of, and keys for looking up, the private information. Given these different uses, and to improve scalability, security and simplicity of administration, the public and private information can be stored in different registries, indeed different types of registry.

3.1. Private Information Registry

The private information required for UAS RID is similar to that required for Internet domain name registration. This facilitates leveraging existing Internet resources, including domain name registration protocols, infrastructure and business models. This implies a further derived requirement: a tm-rid UAS ID MUST be amenable to handling as an Internet domain name (at an arbitrary level in the heirarchy), MUST be registered in at least a pseudo-domain (e.g. .ip6 for reverse lookup), and MAY be registered as a sub-domain (for forward lookup).

A tm-rid private information registry MUST support essential Internet domain name registry operations (e.g. add, delete, update, query) using interoperable open standard protocols. It SHOULD support the Extensible Provisioning Protocol (EPP) and the Registry Data Access Protocol (RDAP) with access controls. It MAY use XACML to specify those access controls. It MUST be listed in a DNS: that DNS MAY be private; but absent any compelling reasons for use of private DNS, SHOULD be the definitive public Internet DNS heirarchy. The tm-rid private information registry in which a given UAS is registered MUST be locatable, starting from the UAS ID, using the methods specified in [RFC7484].

3.2. Public Information Registry

The public information required to be made available by UAS RID is transmitted as clear plaintext to local observers in Broadcast RID and is served to a client by a NETDP in Network RID. Therefore, while IETF can offer e.g. [RFC6280] as one way to implement Network RID, the only public information required to support essential tm-

rid functions for UAS RID is that required to look up Internet domain hosts, services, etc.

A tm-rid public information registry MUST be a standard DNS server, in the definitive public Internet DNS heirarchy. It MUST support NS, MX, SRV, TXT, AAAA, PTR, CNAME and HIP RR types.

3.3. CS-RID SDSP

A CS-RID SDSP MUST appear (i.e. present the same interface) to a NETSP as a NETDP. A CS-RID SDSP MUST appear to a NETDP as a NETSP. A CS-RID SDSP MUST NOT present a standard GCS-facing interface as if it were a NETSP. A CS-RID SDSP MUST NOT present a standard client-facing interface as if it were a NETDP. A CS-RID SDSP MUST present a TBD interface to a CS-RID Finder; this interface SHOULD be based upon but readily distinguishable from that between a GCS and a NETSP.

3.4. CS-RID Finder

A CS-RID Finder MUST present a TBD interface to a CS-RID SDSP; this interface SHOULD be based upon but readily distinguishable from that between a GCS and a NETSP. A CS-RID Finder must implement, integrate or accept outputs from a Broadcast RID receiver. A CS-RID Finder MUST NOT interface directly with a GCS, NETSP, NETDP or Network RID client.

4. Identifiers

A tm-rid UAS ID MUST be a HHIT. It SHOULD be self-generated by the UAS (either UA or GCS) and MUST be registered with the Private Information Registry identified in its heirarchy fields. Each UAS ID HHIT MUST NOT be used more than once, with one exception as follows.

Each UA MAY be assigned, by its manufacturer, a single HI and derived HHIT encoded as a hardware serial number per [CTA2063A]. Such a static HHIT SHOULD be used only to bind one-time use UAS IDs (other HHITs) to the unique UA. Depending upon implementation, this may leave a HI private key in the posession of the manufacturer (see Security Considerations).

Each UA equipped for Broadcast RID MUST be provisioned not only with its HHIT but also with the HI public key from which the HHIT was derived and the corresponding private key, to enable message signature. Each UAS equipped for Network RID MUST be provisioned likewise; the private key SHOULD reside only in the ultimate source of Network RID messages (i.e. on the UA itself if the GCS is merely relaying rather than sourcing Network RID messages). Each observer device MUST be provisioned with public keys of the UAS RID root

registries and MAY be provisioned with public keys or certificates for subordinate registries.

Operators and Private Information Registries MUST possess and other UTM entities MAY possess UAS ID style HHITs. When present, such HHITs SHOULD be used with HIP to strongly mutually authenticate and optionally encrypt communications.

5. Transactions

Each Operator MUST generate a "HIo" and derived "HHITo", register them with a Private Information Registry along with whatever Operator data (inc. PII) is required by the cognizant CAA and the registry, and obtain a certificate "Cro" signed with "HIr(priv)" proving such registration.

To add an UA, an Operator MUST generate a "HIa" and derived "HHITa", create a certificate "Coa" signed with "HIo(priv)" to associate the UA with its Operator, register them with a Private Information Registry along with whatever UAS data is required by the cognizant CAA and the registry, obtain a certificate "Croa" signed with "HIr(priv)" proving such registration, and obtain a certificate "Cra" signed with "HIr(priv)" proving UA registration in that specific registry while preserving Operator privacy. The operator then MUST provision the UA with "HIa", "HIa(priv)", "HHITa" and "Cra".

UA engaging in Broadcast RID MUST use "HIa(priv)" to sign Auth Messages and MUST periodically broadcast "Cra". UAS engaging in Network RID MUST use "HIa(priv)" to sign Auth Messages. Observers MUST use "HIa" from received "Cra" to verify received Broadcast RID Auth messages. Observers without Internet connectivity MAY use "Cra" to identify the trust class of the UAS based on known registry vetting. Observers with Internet connectivity MAY use "HHITa" to perform lookups in the Public Information Registry and MAY then query the Private Information Registry, which MUST enforce access control policy on Operator PII and other sensitive information.

6. IANA Considerations

It is likely that an IPv6 prefix will be needed for the HHIT (or other identifier) space; this will be specified in other drafts.

7. Security Considerations

UAS RID is all about safety and security, so content pertaining to such is not limited to this section. The security provided by asymmetric cryptographic techniques depends upon protection of the private keys. A manufacturer that embeds a private key in an UA may have retained a copy. A manufacturer whose UA are configured by a

closed source application on the GCS which communicates over the Internet with the factory may be sending a copy of a UA or GCS self-generated key back to the factory. Compromise of a registry private key could do widespread harm. Key revocation procedures are as yet to be determined. These risks are in addition to those involving Operator key management practices.

8. Acknowledgments

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

9. References

9.1. Normative References

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

[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>.

[RFC7484] Blanchet, M., "Finding the Authoritative Registration Data (RDAP) Service", RFC 7484, DOI 10.17487/RFC7484, March 2015, <https://www.rfc-editor.org/info/rfc7484>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <https://www.rfc-editor.org/info/rfc8005>.

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

9.2. Informative References

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

[I-D.moskowitz-hip-hierarchical-hit] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-03,

16 December 2019, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-03>.

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

[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>.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, DOI 10.17487/RFC6280, July 2011, <https://www.rfc-editor.org/info/rfc6280>.

[WK65041] ASTM, "Standard Specification for Remote ID and Tracking", September 2019.

Authors' Addresses

Stuart W. Card
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