drip                                                            S. Card
Internet-Draft                                         A. Wiethuechter
Intended status: Informational                           AX Enterprize
Expires: 23 August 2021                                   R. Moskowitz
                                                         HTT Consulting
                                                        S. Zhao (Editor)
                                                                Tencent
                                                              A. Gurtov
                                                   Linkoeping University
                                                       19 February 2021

# Drone Remote Identification Protocol (DRIP) Architecture
**draft-ietf-drip-arch-09**

Abstract

   This document defines an architecture for protocols and services to
   support Unmanned Aircraft System Remote Identification and tracking
   (UAS RID), plus RID-related communications, including required
   architectural building blocks and their interfaces.

Status of This Memo

Copyright Notice

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

Table of Contents

## [1](#). Introduction

This document describes an architecture for protocols and services to support Unmanned Aircraft System Remote Identification and tracking (UAS RID), plus RID-related communications, conforming to proposed and final regulations plus external technical standards, satisfying the requirements listed in the companion requirements document [I-D.ietf-drip-reqs].

Many considerations (especially safety) dictate that UAS be remotely identifiable. Civil Aviation Authorities (CAAs) worldwide are mandating Unmanned Aircraft Systems (UAS) Remote Identification (RID). CAAs currently (2020) promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

### [1.1](#). Overview UAS Remote ID (RID) and RID Standardization

A RID is an application enabler for a UAS to be identified by a UTM/USS or third parties entities such as law enforcement. Many safety and other considerations dictate that UAS be remotely identifiable. CAAs worldwide are mandating UAS RID. The European Union Aviation Safety Agency (EASA) has published [Delegated] and [Implementing] Regulations. The 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.

FAA

The United States Federal Aviation Administration (FAA) has published "Remote Identification of Unmanned Aircraft" [FAA_RID]. CAAs currently promulgate performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed the new ASTM [F3411-19] Standard Specification for Remote ID and Tracking.

ASTM defines one set of RID information and two means, MAC-layer broadcast and IP-layer network, of communicating it. If a UAS uses both communication methods, generally the same information must be provided via both means. The [F3411-19] is cited by FAA in its RID final rule [FAA_RID] as "one potential means of compliance" to a Remote ID rule.

3GPP

   With release 16, 3GPP completed the UAS RID requirement study
   [TS-22.825] and proposed use cases in the mobile network and the
   services that can be offered based on RID.  Release 17
   specification works on enhanced UAS service requirements and
   provides the protocol and application architecture support which
   is applicable for both 4G and 5G network.

## 1.2.  Overview of Types of UAS Remote ID

### 1.2.1.  Broadcast RID

A set of RID messages are defined for direct, one-way, broadcast
transmissions from the UA over Bluetooth or Wi-Fi.  These are
currently defined as MAC-Layer messages.  Internet (or other Wide
Area Network) connectivity is only needed for UAS registry
information lookup by observers using the locally directly received
UAS RID as a key.  Broadcast RID should be functionally usable in
situations with no Internet connectivity.

The Broadcast RID is illustrated in Figure 1 below.

```
                 x x   UA
               xxxxx
                 |
                 |
                 |      app messages directly over
                 |      one-way RF data link (no IP)
                 |
                 |
                 +
                 x
               xxxxx
                 x
                 x
                 x x    Observer's device (e.g. smartphone)
               x    x


                            Figure 1
```

With Broadcast RID, an Observer is limited to their radio "visible"
airspace for UAS awareness and information.  With Internet queries
using harvested RID, the Observer may gain more information about
those visible UAS.

## 1.2.2.  Network RID

A RID data dictionary and data flow for Network RID are defined in
[F3411-19].  This data flow is from a UAS via unspecified means (but
at least in part over the Internet) to a Network Remote ID Service
Provider (Net-RID SP).  These Net-RID SPs provide the RID data
information to Network Remote ID Display Providers (Net-RID DP).  It
is the Net-RID DP that responds to queries from Network Remote ID
observers (expected typically, but not specified exclusively, to be
web-based) specifying airspace volumes of interest.  Network RID
depends upon connectivity, in several segments, via the Internet,
from the UAS to the observer.

The Network RID is illustrated in Figure 2 below:

```
        x x   UA
        xxxxx        *******************
          |   \     *                   ------*---+------------+
          |    \    *             /        *  | NET_RID_SP |
          |     \   * ------------/    +---*--+------------+
          | RF    \ */                 |    *
          |        *       INTERNET    |    *   +------------+
          |       /*                   +---*--| NET_RID_DP |
          |      / *                   +---*--+------------+
          +     /   *                  |    *
           x   /     ****************|***      x
          xxxxx                      |        xxxxx
           x                         +-------   x
           x                                    x
          x x    Operator (GCS)       Observer  x x
          x   x                                x   x
```

                            Figure 2

Via the direct Radio Frequency (RF) link between the UA and GCS,
Command and Control (C2) flows between the GCS to the UA such that
either can communicate with the Net-RID SP.  For all but the simplest
hobby aircraft, position and status flow from the UA to the GCS and
on to the Net-RID SP.  Thus via the Internet, through three distinct
segments, Network RID information flows from the UAS to the Observer.

        Informative note: The RF link between UA and GCS is not in
        scope of the Network RID.

## 1.3.  Overview of USS Interoperability

   Each UAS is registered to at least one USS.  With Net-RID, there is
   direct communication between the UAS and its USS.  With Broadcast-
   RID, the UAS Operator has either pre-filed a 4D space volume for USS
   operational knowledge and/or Observers can be providing information
   about observed UA to a USS.  USS exchange information via a Discovery
   and Synchronization Service (DSS) so all USS have knowledge about all
   activities in a 4D airspace.  The interactions among observer, UA,
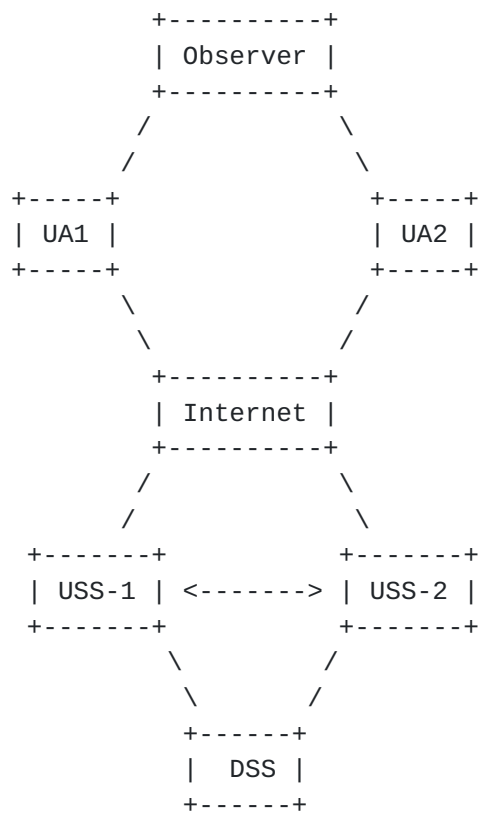   and USS is shown in Figure 3.

```
                        +----------+
                        | Observer |
                        +----------+
                        /          \
                       /            \
                  +-----+            +-----+
                  | UA1 |            | UA2 |
                  +-----+            +-----+
                      \              /
                       \            /
                        +----------+
                        | Internet |
                        +----------+
                        /          \
                       /            \
                  +-------+          +-------+
                  | USS-1 | <------> | USS-2 |
                  +-------+          +-------+
                          \          /
                           \        /
                        +------+
                        | DSS |
                        +------+
```

                         Figure 3

## 1.4.  Overview of DRIP Architecture

   The requirements document [I-D.ietf-drip-reqs] also provides an
   extended introduction to the problem space, use cases, etc.  Only a
   brief summary of that introduction will be restated here as context,
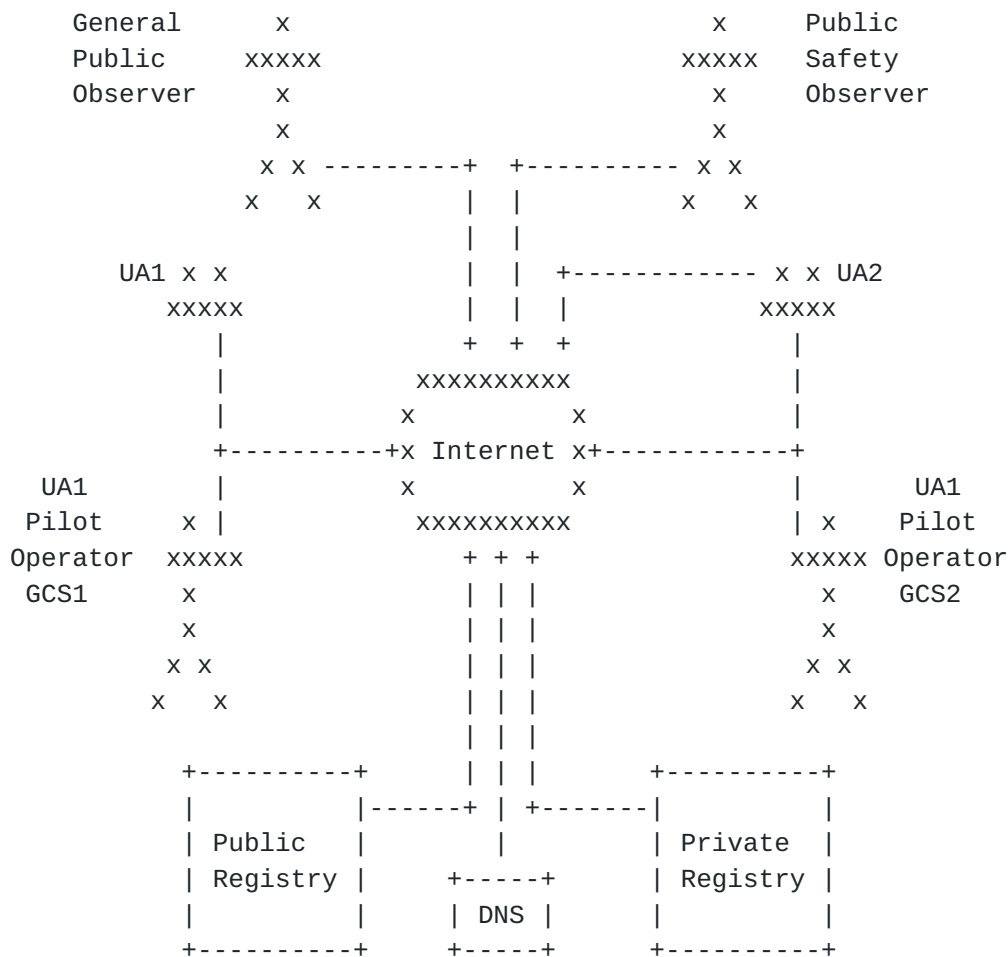   with reference to the general architecture shown in Figure 4 below.

```
          General      x                            x      Public
          Public    xxxxx                        xxxxx   Safety
          Observer     x                            x      Observer
                       x                            x
                 x x ---------+   +---------- x x
                  x    x       |   |          x    x
                              |   |
          UA1 x x            |   |  +----------- x x UA2
              xxxxx          |   |  |               xxxxx
                |            +   +  +               |
                |             xxxxxxxxxx            |
                |              x          x         |
              +----------+x Internet x+------------+
          UA1       |        x          x          |        UA1
         Pilot   x |         xxxxxxxxxx            | x     Pilot
        Operator  xxxxx         + + +              xxxxx Operator
         GCS1      x            | | |                x     GCS2
                   x            | | |                x
                  x x           | | |               x x
                 x    x         | | |              x    x
                               | | |
             +----------+      | | |        +----------+
             |          |------+ | +-------|          |
             | Public   |        |         | Private  |
             | Registry |     +-----+      | Registry |
             |          |     | DNS |      |          |
             +----------+     +-----+      +----------+
```

                              Figure 4

   DRIP will enable leveraging existing Internet resources (standard
   protocols, services, infrastructure, and business models) to meet UAS
   RID and closely related needs.  DRIP will specify how to apply IETF
   standards, complementing [F3411-19] and other external standards, to
   satisfy UAS RID requirements.  DRIP will update existing and develop
   new protocol standards as needed to accomplish the foregoing.

   This document will outline the UAS RID architecture into which DRIP
   must fit and the architecture for DRIP itself.  This includes
   presenting the gaps between the CAAs' Concepts of Operations and
   [F3411-19] as it relates to the use of Internet technologies and UA
   direct RF communications.  Issues include, but are not limited to:

      -  Design of trustworthy remote ID and trust in RID messages
         (Section 4)

- Mechanisms to leverage Domain Name System (DNS: [RFC1034]) and Extensible Provisioning Protocol (EPP [RFC5731]) technology to provide for private (Section 5.2) and public (Section 5.1) Information Registry.

- Harvesting broadcast remote ID messages for UTM inclusion (Section 6)

- Trustworthy RID Transactions (Section 7)

- Privacy in RID messages (PII protection) ((Section 8))

## 2.  Conventions

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 above.

## 3.  Definitions and Abbreviations

## 3.1.  Additional Definitions

This document uses terms defined in [I-D.ietf-drip-reqs].

## 3.2.  Abbreviations

ADS-B:      Automatic Dependent Surveillance Broadcast

DSS:        Discovery & Synchronization Service

EdDSA:      Edwards-Curve Digital Signature Algorithm

GCS:        Ground Control Station

HHIT:       Hierarchical HIT Registries

HIP:        Host Identity Protocol

HIT:        Host Identity Tag

RID:        Remote ID

Net-RID SP: Network RID Service Provider

Net-RID DP: Network RID Display Provider.

   PII:        Personally Identifiable Information

   RF:         Radio Frequency

   SDSP:       Supplemental Data Service Provider

   UA:         Unmanned Aircraft

   UAS:        Unmanned Aircraft System

   USS:        UAS Service Supplier

   UTM:        UAS Traffic Management

## 3.3.  Claims, Assertions, Attestations, and Certificates

   This section introduces the meaning of "Claims", "Assertions",
   "Attestations", and "Certificates" in the context of DRIP.

   This is due, in part, to the term "certificate" having significant
   technologic and legal baggage associated with it, specifically around
   X.509 certificates.  These type of certificates and Public Key
   Infrastructure invokes more legal and public policy considerations
   than probably any other electronic communication sector.  It emerged
   as a governmental platform for trusted identity management and was
   pursued in intergovernmental bodies with links into treaty
   instruments.  As such the following terms are being used in DRIP.

   Claims:

      For DRIP claims are used in the form of a predicate (X is Y, X has
      property Y, and most importantly X owns Y).  The basic form of a
      claim is an entity using a HHIT as an identifier in the DRIP UAS
      system.

   Assertions:

      Assertions, under DRIP, are defined as being a set of one or more
      claims.  This definition is borrowed from JWT/CWT.  An HHIT in of
      itself can be seen as a set of assertions.  First that the
      identifier is a handle to an asymmetric keypair owned by the
      entity and that it also is part of the given registry (specified
      by the HID).

   Attestations:

An attestation is a signed claim.  The signee may be the claimant themselves or a third party.  Under DRIP this is normally used when a set of entities asserts a relationship between them along with other information.

Certificates:

Certificates in DRIP have a narrow definition of being signed exclusively by a third party and are only over identities.

## [4](#). HHIT for UAS Remote ID

This section describes the basic requirements of a DRIP UAS remote ID per regulation constrains from ASTM [[F3411-19](#)] and explains the use of Hierarchical Host Identity Tags (HHITs) as self-asserting IPv6 addresses and thereby a trustable Identifier for use as the UAS Remote ID.  HHITs self-attest to the included explicit hierarchy that provides Registrar discovery for 3rd-party ID attestation.

### [4.1](#). UAS Remote Identifiers Problem Space

A DRIP UAS ID needs to be "Trustworthy".  This means that within the framework of the RID messages, an observer can establish that the RID used does uniquely belong to the UA.  That the only way for any other UA to assert this RID would be to steal something from within the UA. The RID is self-generated by the UAS (either UA or GCS) and registered with the USS.

The data communication of using Broadcast RID faces extreme challenges due to the limitation set by regulations.  The ASTM [[F3411-19](#)] defines the Basic RID message which is expected to contain certain RID data and the Authentication message.  The Basic RID message has a maximum payload of 25 bytes and the maximum size allocated by ASTM for the RID is 20 bytes and only 3 bytes are left unused.  currently, the authentication maximum payload is defined to be 224 bytes.

Standard approaches like X.509 and PKI will not fit these constraints, even using the new EdDSA An example of a technology that will fit within these limitations is an enhancement of the Host Identity Tag (HIT) of HIPv2 [[RFC8032](#)] algorithm.[[RFC7401](#)] using Hierarchical HITs (HHITs) for UAS RID is outlined in HHIT based UAS RID [[I-D.ietf-drip-rid](#)].  As PKI with X.509 is being used in other systems with which UAS RID must interoperate (e.g. the UTM Discovery and Synchronization Service and the UTM InterUSS protocol) mappings between the more flexible but larger X.509 certificates and the HHIT based structures must be devised.

By using the EdDSA HHIT suite, the self-assertions of the RID can be
done in as little as 84 bytes.  Third-party assertions can be done in
200 bytes.  An observer would need Internet access to validate a
self-assertion claim.  A third-party assertion can be validated via a
small credential cache in a disconnected environment.  This third-
party assertion is possible when the third-party also uses HHITs for
its identity and the UA has the public key for that HHIT.

## 4.2.  HIT as A Trustworthy UAS Remote ID

For a Remote ID to be trustworthy in the Broadcast mode, there MUST
be an asymmetric keypair for proof of ID ownership.  The common
method of using a key signing operation to assert ownership of an ID,
does not guarantee name uniqueness.  Any entity can sign an ID,
claiming ownership.  To mitigate spoofing risks, the ID needs to be
cryptographically generated from the public key, in such a manner
that it is statistically hard for an entity to create a public key
that would generate (spoof) the ID.  Thus the signing of such an ID
becomes an attestation (compared to claim) of ownership.

HITs are statistically unique through the cryptographic hash feature
of second-preimage resistance.  The cryptographically-bound addition
of the Hierarchy and a HHIT registration process (e.g. based on
Extensible Provisioning Protocol, [RFC5730]) provide complete, global
HHIT uniqueness.  This is in contrast to general IDs (e.g. a UUID or
device serial number) as the subject in an X.509 certificate.

## 4.3.  HHIT for Remote ID Registration and Lookup

Remote IDs need a deterministic lookup mechanism that rapidly
provides actionable information about the identified UA.  The ID
itself needs to be the inquiry input into the lookup given the
constraints imposed by some of the broadcast media.  This can best be
achieved by an ID registration hierarchy cryptographically embedded
within the ID.

The HHIT needs to consist of a registration hierarchy, the hashing
crypto suite information, and the hash of these items along with the
underlying public key.  Additional information, e.g. an IPv6 prefix,
may enhance the HHITs use beyond the basic Remote ID function (e.g.
use in HIP, [RFC7401]).

A DRIP UAS ID SHOULD be a HHIT.  It SHOULD be self-generated by the
UAS (either UA or GCS) and MUST be registered with the Private
Information Registry (More details in Section 5.2) identified in its
hierarchy 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 possession 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.

## 4.4.  HHIT for Remote ID Encryption

The only (at time of Trustworthy Remote ID design) extant fixed
length ID cryptographically derived from a public key are the Host
Identity Tag [RFC7401], HITs, and Cryptographically Generated
Addresses [RFC3972], CGAs.  Both lack a registration/retrieval
capability and CGAs have only a limited crypto agility [RFC4982].
Distributed Hash Tables have been tried for HITs [RFC6537]; this is
really not workable for a globally deployed UAS Remote ID scheme.

The security of HHITs is achieved first through the cryptographic
hashing function of the above information, along with a registration
process to mitigate the probability of a hash collision (first
registered, first allowed).

## 5.  DRIP HHIT RID Registration and Registries

The DRIP HHIT RID registration goes beyond what is currently
envisioned in UTM for the UAS to USS registration/subscription
process.

   UAS registries hold both public and private UAS information resulting
   from the UAS RID registration.  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.

## 5.1.  Public Information Registry

### 5.1.1.  Background

   The public registry provides trustable information such as
   attestations of RID ownership and HDA registration.  Optionally,
   pointers to the repositories for the HDA and RAA implicit in the RID
   can be included (e.g. for HDA and RAA HHIT|HI used in attestation
   signing operations).  This public information will principally used
   by observers of Broadcast RID messages.  Data on UAS that only use
   Network RID, is only available via an observer's Net-RID DP that
   would tend to directly provide all public registry information
   directly.  The observer may visually "see" these UAS, but they are
   silent to the observer; the Net-RID DP is the only source of
   information based on a query for an airspace volume.  Thus there is
   no need for information on them in a Public Registry.

### 5.1.2.  Proposed Approach

   A DRIP public information registry MUST respond to standard DNS
   queries, in the definitive public Internet DNS hierarchy.  It MUST
   support NS, MX, SRV, TXT, AAAA, PTR, CNAME and HIP RR (the last per
   [RFC8005]) types.  If a DRIP public information registry lists, in a
   HIP RR, any HIP RVS servers for a given DRIP UAS ID, those RVS
   servers MUST restrict relay services per AAA policy; this may require
   extensions to [RFC8004].  These public information registries SHOULD
   use secure DNS transport (e.g.  DNS over TLS) to deliver public
   information that is not inherently trustable (e.g. everything other
   than attestations).

## 5.2.  Private Information Registry

### 5.2.1.  Background

   The private information required for DRIP RID is similar to that
   required for Internet domain name registration.  This information
   SHOULD be available for ALL UAS, including those that only use
   Network RID.  A DRIP RID solution can leverage existing Internet
   resources: registration protocols, infrastructure and business
   models, by fitting into an ID structure compatible with DNS names.
   This implies some sort of hierarchy, for scalability, and management
   of this hierarchy.  It is expected that the private registry function

will be provided by the same organizations that run USS, and likely
integrated with USS.

## 5.2.2.  Proposed Approach

A DRIP RID MUST be amenable to handling as an Internet domain name
(at an arbitrary level in the hierarchy), MUST be registered in at
least a pseudo-domain (e.g. .ip6.arpa for reverse lookup), and MAY be
registered as a sub-domain (for forward lookup).  This DNS
information MAY be protected with DNSSEC.  Its access SHOULD be
protected with a secure DNS transport (e.g.  DNS over TLS).

A DRIP 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 hierarchy.  The DRIP
private information registry in which a given UAS is registered MUST
be findable, starting from the UAS ID, using the methods specified in
[RFC7484].  A DRIP private information registry MAY support WebFinger
as specified in [RFC7033].

## 6.  Harvesting Broadcast Remote ID messages for UTM Inclusion

ASTM anticipated that regulators would require both Broadcast RID and
Network RID for large UAS, but allow RID requirements for small UAS
to be satisfied with the operator's choice of either Broadcast RID or
Network RID.  The EASA initially specified Broadcast RID for UAS of
essentially all UAS and is now also considering Network RID.  The FAA
RID Final Rules only specifies Broadcast RID for UAS.

One obvious opportunity is to enhance the architecture with gateways
from Broadcast RID to Network RID.  This provides the best of both
and gives regulators and operators flexibility.  It offers
considerable enhancement over some Network RID options such as only
reporting planned 4D operation space by the operator.

These gateways could be pre-positioned (e.g. around airports, public
gatherings, and other sensitive areas) and/or crowd-sourced (as
nothing more than a smartphone with a suitable app is needed).  As
Broadcast RID media have limited range, gateways receiving messages
claiming locations far from the gateway can alert authorities or a
SDSP to the failed sanity check possibly indicating intent to
deceive.  Surveillance SDSPs can use messages with precise date/time/
position stamps from the gateways to multilaterate UA location,

independent of the locations claimed in the messages (which may have
a natural time lag as it is), which are entirely operator self-
reported in UAS RID and UTM.

Further, gateways with additional sensors (e.g. smartphones with
cameras) can provide independent information on the UA type and size,
confirming or refuting those claims made in the RID messages.  This
Crowd Sourced Remote ID (CS-RID) would be a significant enhancement,
beyond baseline DRIP functionality; if implemented, it adds two more
entity types.

## 6.1.  The CS-RID Finder

A CS-RID Finder is the gateway for Broadcast Remote ID Messages into
the UTM.  It performs this gateway function via a CS-RID SDSP.  A CS-
RID Finder must implement, integrate, or accept outputs from, a
Broadcast RID receiver.  It MUST NOT interface directly with a GCS,
Net-RID SP, Net-RID DP or Network RID client.  It 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 Net-RID SP.

## 6.2.  The CS-RID SDSP

A CS-RID SDSP MUST appear (i.e. present the same interface) to a Net-
RID SP as a Net-RID DP.  A CS-RID SDSP MUST appear to a Net-RID DP as
a Net-RID SP.  A CS-RID SDSP MUST NOT present a standard GCS-facing
interface as if it were a Net-RID SP.  A CS-RID SDSP MUST NOT present
a standard client-facing interface as if it were a Net-RID DP.  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 Net-RID SP.

## 7.  DRIP Transactions Enabling Trustworthy

The UTM (U-SPACE) architecture leaves much about all the operators/
UAS to the various USS.  Each CAA will have some registration
requirements on operators (FAA part 105 is considered very minimal by
some CAA), along with some UAS and operation registration.  DRIP
leverages this model with Identities for each component that augment
the DRIP RID and transactions to support these Identities.

To this end, in DRIP, each Operator MUST generate a Host Identity of
the Operator (HIo) and derived Hierarchical HIT of the Operator
(HHITo).  These are registered with a Private Information Registry
along with whatever Operator data (inc.  PII) is required by the
cognizant CAA and the registry.  In response, the Operator will
obtain a Certificate from the Registry, an Operator (Cro), signed
with the Host Identity of the Registry private key (HIr(priv))
proving such registration.

An Operator may now add a UA.

*  An Operator MUST generate a Host Identity of the Aircraft (HIa)
   and derived Hierarchical HIT of the Aircraft (HHITa)

*  Create a Certificate from the Operator on the Aircraft (Coa)
   signed with the Host Identity of the Operator private key
   (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 from the Registry on the Operator and
   Aircraft ("Croa") signed with the HIr(priv) proving such
   registration

*  And obtain a Certificate from the Registry on the Aircraft (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 AAA policy on
      Operator PII and other sensitive information

## 8.  Privacy for Broadcast PII

   Broadcast RID messages may contain PII.  A viable architecture for
   PII protection would be symmetric encryption of the PII using a key
   known to the UAS and its USS.  An authorized Observer may send the
   encrypted PII along with the Remote ID (to their UTM Service
   Provider) to get the plaintext.  Alternatively, the authorized
   Observer may receive the key to directly decrypt all future PII
   content from the UA.

   PII SHOULD protected unless the UAS is informed otherwise.  This may
   come from operational instructions to even permit flying in a space/
   time.  It may be special instructions at the start or during an
   operation.  PII protection should not be used if the UAS loses
   connectivity to the USS.  The UAS always has the option to abort the
   operation if PII protection is disallowed.

   An authorized observer may instruct a UAS via the USS that conditions
   have changed mandating no PII protection or land the UA (abort the
   operation).

## 9.  Security Considerations

   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.  Keys may be
   extracted from a GCS or UA; the RID sender of a small harmless UA (or
   the entire UA) could be carried by a larger dangerous UA as a "false
   flag."  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.

## 10.  Acknowledgements

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 DRIP WG efforts.  The work of ASTM F38.02 in
balancing the interests of diverse stakeholders is essential to the
necessary rapid and widespread deployment of UAS RID.  IETF
volunteers who have contributed to this draft include Amelia
Andersdotter and Mohamed Boucadair.

## 11.  References

### 11.1.  Normative References

[I-D.ietf-drip-reqs]
          Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov,
          "Drone Remote Identification Protocol (DRIP)
          Requirements", Work in Progress, Internet-Draft, draft-
          ietf-drip-reqs-06, 1 November 2020, <http://www.ietf.org/
          internet-drafts/draft-ietf-drip-reqs-06.txt>.

[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>.

[RFC8032]  Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital
          Signature Algorithm (EdDSA)", RFC 8032,
          DOI 10.17487/RFC8032, January 2017,
          <https://www.rfc-editor.org/info/rfc8032>.

[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>.

### 11.2.  Informative References

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

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

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

   [FAA_RID]   United States Federal Aviation Administration (FAA),
               "Remote Identification of Unmanned Aircraft", 2021,
               <https://www.govinfo.gov/content/pkg/FR-2021-01-15/
               pdf/2020-28948.pdf>.

   [I-D.ietf-drip-rid]
               Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov,
               "UAS Remote ID", Work in Progress, Internet-Draft, draft-
               ietf-drip-rid-06, 31 December 2020, <http://www.ietf.org/
               internet-drafts/draft-ietf-drip-rid-06.txt>.

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

   [LAANC]     United States Federal Aviation Administration (FAA), "Low
               Altitude Authorization and Notification Capability", n.d.,
               <https://www.faa.gov/uas/programs_partnerships/
               data_exchange/>.

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

   [RFC1034]   Mockapetris, P., "Domain names - concepts and facilities",
               STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987,
               <https://www.rfc-editor.org/info/rfc1034>.

   [RFC3972]   Aura, T., "Cryptographically Generated Addresses (CGA)",
               RFC 3972, DOI 10.17487/RFC3972, March 2005,
               <https://www.rfc-editor.org/info/rfc3972>.

   [RFC4982]   Bagnulo, M. and J. Arkko, "Support for Multiple Hash
               Algorithms in Cryptographically Generated Addresses
               (CGAs)", RFC 4982, DOI 10.17487/RFC4982, July 2007,
               <https://www.rfc-editor.org/info/rfc4982>.

   [RFC5730]   Hollenbeck, S., "Extensible Provisioning Protocol (EPP)",
               STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009,
               <https://www.rfc-editor.org/info/rfc5730>.

   [RFC5731]   Hollenbeck, S., "Extensible Provisioning Protocol (EPP)
               Domain Name Mapping", STD 69, RFC 5731,
               DOI 10.17487/RFC5731, August 2009,
               <https://www.rfc-editor.org/info/rfc5731>.

   [RFC6537]  Ahrenholz, J., "Host Identity Protocol Distributed Hash
              Table Interface", RFC 6537, DOI 10.17487/RFC6537, February
              2012, <https://www.rfc-editor.org/info/rfc6537>.

   [RFC7033]  Jones, P., Salgueiro, G., Jones, M., and J. Smarr,
              "WebFinger", RFC 7033, DOI 10.17487/RFC7033, September
              2013, <https://www.rfc-editor.org/info/rfc7033>.

   [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>.

   [RFC8004]  Laganier, J. and L. Eggert, "Host Identity Protocol (HIP)
              Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004,
              October 2016, <https://www.rfc-editor.org/info/rfc8004>.

   [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>.

   [TS-22.825]
              3GPP, "UAS RID requirement study", n.d.,
              <https://portal.3gpp.org/desktopmodules/Specifications/
              SpecificationDetails.aspx?specificationId=3527>.

   [U-Space]  European Organization for the Safety of Air Navigation
              (EUROCONTROL), "U-space Concept of Operations", 2019,
              <https://www.sesarju.eu/sites/default/files/documents/u-
              space/CORUS%20ConOps%20vol2.pdf>.

Appendix A.  Overview of Unmanned Aircraft Systems (UAS) Traffic

### A.1.  Operation Concept

   The National Aeronautics and Space Administration (NASA) and FAAs'
   effort of integrating UAS's operation into the national airspace
   system (NAS) leads to the development of the concept of UTM and the
   ecosystem around it.  The UTM concept was initially presented in
   2013.  The eventual development and implementation are conducted by
   the UTM research transition team which is the joint workforce by FAA
   and NASA.  World efforts took place afterward.  The Single European
   Sky ATM Research (SESAR) started the CORUS project to research its
   UTM counterpart concept, namely [U-Space].  This effort is led by the
   European Organization for the Safety of Air Navigation (Eurocontrol).

   Both NASA and SESAR have published the UTM concept of operations to
   guide the development of their future air traffic management (ATM)
   system and make sure safe and efficient integrations of manned and
   unmanned aircraft into the national airspace.

   The UTM composes of UAS operation infrastructure, procedures and
   local regulation compliance policies to guarantee UAS's safe
   integration and operation.  The main functionality of a UTM includes,
   but is not limited to, providing means of communication between UAS
   operators and service providers and a platform to facilitate
   communication among UAS service providers.

### A.2.  UAS Service Supplier (USS)

   A USS plays an important role to fulfill the key performance
   indicators (KPIs) that a UTM has to offer.  Such Entity acts as a
   proxy between UAS operators and UTM service providers.  It provides
   services like real-time UAS traffic monitor and planning,
   aeronautical data archiving, airspace and violation control,
   interacting with other third-party control entities, etc.  A USS can
   coexist with other USS(s) to build a large service coverage map which
   can load-balance, relay and share UAS traffic information.

   The FAA works with UAS industry shareholders and promotes the Low
   Altitude Authorization and Notification Capability [LAANC] program
   which is the first implementation to realize UTM's functionality.
   The LAANC program can automate the UAS's fly plan application and
   approval process for airspace authorization in real-time by checking
   against multiple aeronautical databases such as airspace
   classification and fly rules associated with it, FAA UAS facility
   map, special use airspace, Notice to airman (NOTAM) and Temporary
   flight rule (TFR).

A.3.  UTM Use Cases for UAS Operations

   This section illustrates a couple of use case scenarios where UAS
   participation in UTM has significant safety improvement.

   1.  For a UAS participating in UTM and takeoff or land in a
       controlled airspace (e.g., Class Bravo, Charlie, Delta and Echo
       in United States), the USS where UAS is currently communicating
       with is responsible for UAS's registration, authenticating the
       UAS's fly plan by checking against designated UAS fly map
       database, obtaining the air traffic control (ATC) authorization
       and monitor the UAS fly path in order to maintain safe boundary
       and follow the pre-authorized route.

   2.  For a UAS participating in UTM and take off or land in an
       uncontrolled airspace (ex.  Class Golf in the United States),
       pre-fly authorization must be obtained from a USS when operating
       beyond-visual-of-sight (BVLOS) operation.  The USS either accepts
       or rejects received intended fly plan from the UAS.  Accepted UAS
       operation may share its current fly data such as GPS position and
       altitude to USS.  The USS may keep the UAS operation status near
       real-time and may keep it as a record for overall airspace air
       traffic monitor.

A.4.  Automatic Dependent Surveillance Broadcast (ADS-B)

   The ADS-B is the de facto technology used in manned aviation for
   sharing location information, which is a ground and satellite based
   system designed in the early 2000s.  Broadcast RID is conceptually
   similar to ADS-B.  However, for numerous technical and regulatory
   reasons, ADS-B itself is not suitable for low-flying small UA.
   Technical reasons include: needing RF-LOS to large, expensive (hence
   scarce) ground stations; needing both a satellite receiver and 1090
   MHz transceiver onboard CSWaP constrained UA; the limited bandwidth
   of both uplink and downlink, which are adequate for the current
   manned aviation traffic volume, but would likely be saturated by
   large numbers of UAS, endangering manned aviation; etc.
   Understanding these technical shortcomings, regulators world-wide
   have ruled out use of ADS-B for the small UAS for which UAS RID and
   DRIP are intended.

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


Shuai Zhao
Tencent
2747 Park Blvd
Palo Alto,  94588
United States of America

Email: shuai.zhao@ieee.org


Andrei Gurtov
Linkoeping University
IDA
SE-58183 Linkoeping Linkoeping
Sweden

Email: gurtov@acm.org