drip Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 February 2026

A. Wiethuechter, Ed.
AX Enterprize, LLC
J. Reid
RTFM llp

19 August 2025

DRIP Entity Tags in the Domain Name System
draft-ietf-drip-registries-33

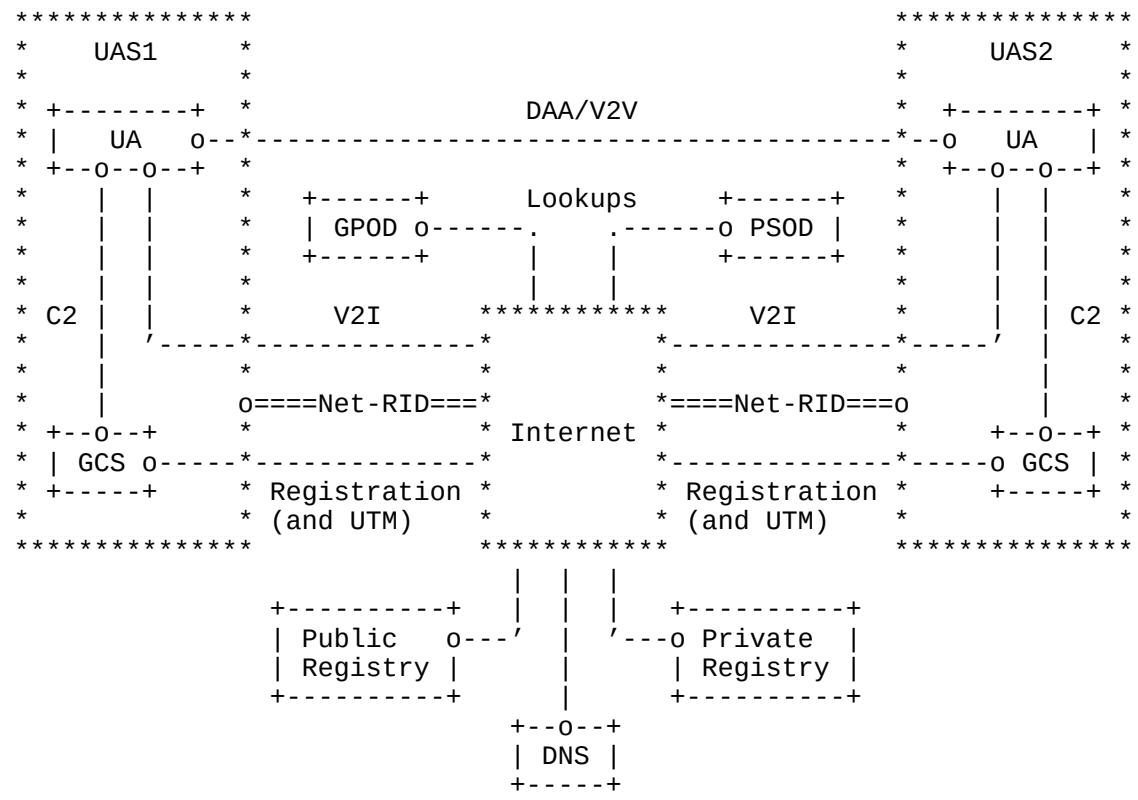
Abstract

This document defines the Domain Name System (DNS) functionality of a Drone Remote Identification Protocol (DRIP) Identity Management Entity (DIME). It is built around DRIP Entity Tags (DETs) to standardize a hierarchical registry structure and associated processes to facilitate trustable and scalable registration and lookup of information related to Unmanned Aircraft Systems (UAS). The registry system supports issuance, discovery, and verification of DETs, enabling secure identification and association of UAS and their operators. It also defines the interactions between different classes of registries (root, organizational, and individual) and their respective roles in maintaining the integrity of the registration data. This architecture enables decentralized, federated operation while supporting privacy, traceability, and regulatory compliance requirements in the context of UAS Remote ID and other services.

Table of Contents

1. Introduction

Registries are fundamental to Unmanned Aircraft System (UAS) Remote Identification (RID). Only very limited operational information can be sent via Broadcast RID, but extended information is sometimes needed. The most essential element of information from RID is the UAS ID, the unique key for lookup of extended information in relevant registries (see Figure 1; Figure 4 of [RFC9434]).



DAA: Detect And Avoid
GPOD: General Public Observer Device
PSOD: Public Safety Observer Device
V2I: Vehicle-to-Infrastructure
V2V: Vehicle-to-Vehicle

Figure 1: Global UAS RID Usage Scenario (Figure 4 of RFC9434)

When a DRIP Entity Tag (DET) [RFC9374] is used as the UAS ID in RID, extended information can be retrieved from a DRIP Identity Management Entity (DIME), which manages registration of and associated lookups from DETs. In this document it is assumed the DIME is a function of UAS Service Suppliers (USS) (Appendix A.2 of [RFC9434]) but a DIME can be independent or handled by another entity as well.

1.1. General Concept

DRIP Entity Tags (DETs) embed a hierarchy scheme which is mapped onto the Domain Name System (DNS) [STD13]. DIMEs enforce registration and information access of data associated with a DET while also providing the trust inherited from being a member of the hierarchy. Other identifiers and their methods are out of scope for this document.

Authoritative Name Servers of the DNS provide the public information such as the cryptographic keys, endorsements and certificates of DETs and pointers to private information resources. Cryptographic (public) keys are used to authenticate anything signed by a DET, such as in the Authentication defined in [RFC9575] for Broadcast RID. Endorsements and certificates are used to endorse the claim of being part of the hierarchy.

This document does not specify AAA mechanisms used by Private Information Registries to store and protect Personally Identifiable Information (PII).

1.2. Scope

The scope of this document is the DNS registration of DETs with the DNS delegation of the reverse domain of IPv6 Prefix, assigned by IANA for DETs 2001:30::/28 and RRsets used to handle DETs.

2. Terminology

2.1. Required 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. Additional Definitions

This document makes use of the terms and abbreviations from previous DRIP documents. Below are subsets, grouped by original document, of terms used this document. Please see those documents for additional context, definitions and any further referenced material.

From Section 2.2 of [RFC9153] this document uses: AAA, CAA, GCS, ICAO, PII, Observer, Operator, UA, UAS, USS, and UTM.

From Section 2 of [RFC9434] this document uses: Certificate, DIME, and Endorsement.

From Section 2 of [RFC9374] this document uses: HDA, HID, and RAA.

3. DET Hierarchy in DNS

[RFC9374] defines the HHIT and further specifies an instance of them used for UAS RID called DETs. The HHIT/DET is a 128-bit value that is as an IPv6 address intended primarily as an identifier rather than locator. Its format is in Figure 2, shown here for reference, and further information is in [RFC9374].

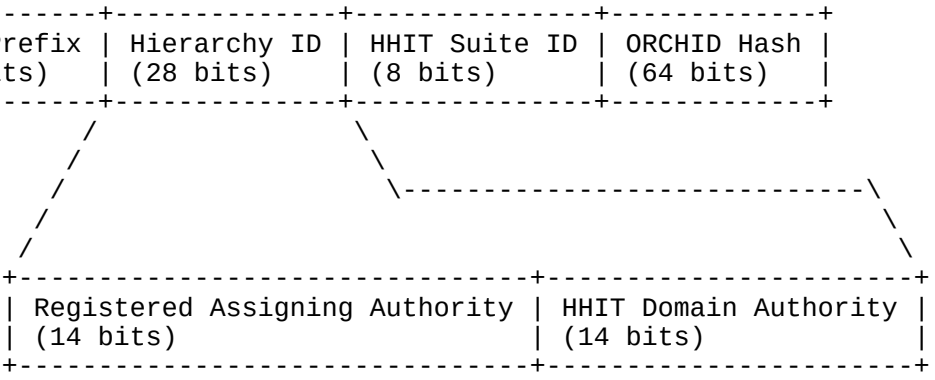


Figure 2: DRIP Entity Tag Breakdown

[RFC9374] assigns the IPv6 prefix 2001:30::/28 for DETs. Its corresponding domain name for reverse lookups is 3.0.0.1.0.0.2.ip6.arpa.. The IAB has administrative control of this domain name.

Due to the nature of the hierarchy split and its relationship to nibble reversing of the IPv6 address (Section 2.5 of [STD88]), the upper level of hierarchy (i.e., Registered Assigning Authority (RAA)) "borrows" the upper two bits of their respective HHIT Domain

Authority (HDA) space for DNS delegation. As such the IPv6 prefix of RAAs are 2001:3x:xxx0::/44 and HDAs are 2001:3x:xxxy:yy00::/56 with respective nibble reverse domains of x.x.x.x.3.0.0.1.0.0.2.ip6.arpa. and y.y.y.x.x.x.x.3.0.0.1.0.0.2.ip6.arpa..

This document preallocates a subset of RAAs based on the ISO 3166-1 Numeric Nation Code [ISO3166-1]. This is to support the initial use case of DETs in UAS RID on an international level. See Section 6.2.1 for the RAA allocations.

The HDA values of 0, 4096, 8192 and 12288 are reserved for operational use of an RAA (a by-product of the above mentioned borrowing of bits), specifically when to register with the apex and endorse delegations of HDAs in their namespace.

The administration, management and policy for the operation of a DIME at any level in the hierarchy (Apex, RAA or HDA) is out of scope for this document. For RAAs or DETs allocated on a per-country basis, these considerations should be be determined by the appropriate national authorities, presumably the Civil Aviation Authority (CAA).

3.1. Use of Existing DNS Models

DRIP relies on the DNS and as such roughly follows the registrant-registrar-registry model. In the UAS ecosystem, the registrant would be the end user who owns/controls the Unmanned Aircraft. They are ultimately responsible for the DET and any other information that gets published in the DNS. Registrants use agents known as registrars to manage their interactions with the registry. Registrars typically provide optional additional services such as DNS hosting.

The registry maintains a database of the registered domain names and their related metadata such as the contact details for domain name holder and the relevant registrar. The registry provides DNS service for the zone apex which contains delegation information for domain names. Registries generally provide services such RDAP [STD95] or equivalent to publish metadata about the registered domain names and their registrants and registrars.

Registrants have contracts with registrars who in turn have contracts with registries. Payments follow this model too: the registrant buys services from a registrar who pays for services provided by the registry.

By definition, there can only be one registry for a domain name. A registry can have an arbitrary number of registrars who compete with each other on price, service and customer support.

3.1.1. DNS Model Considerations for DIMEs

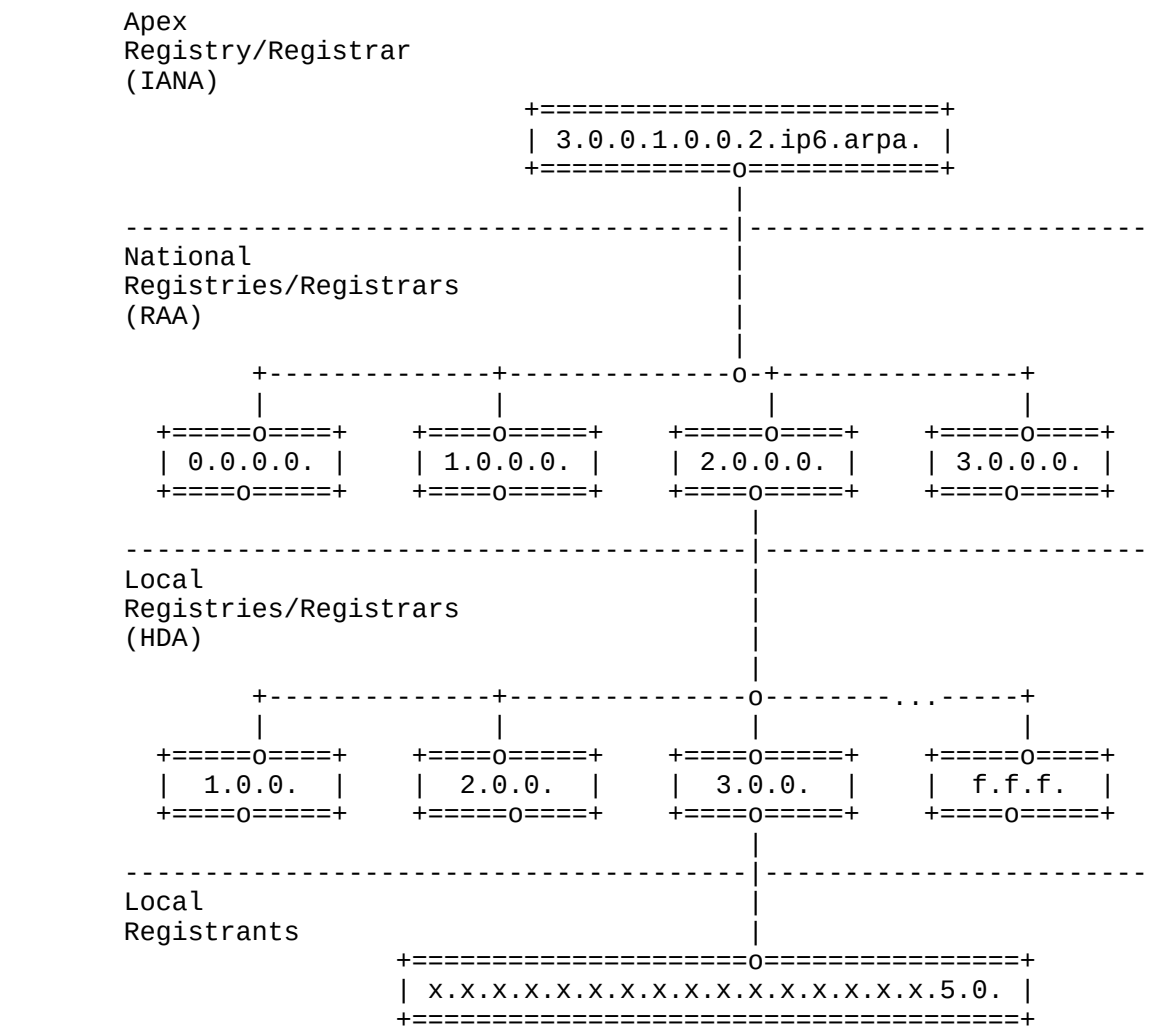


Figure 3: Example DRIP DNS Model

While the registrant-registrar-registry model is mature and well understood, it may not be appropriate for DRIP registrations in some circumstances. It could add costs and complexity; developing policies and contracts as outlined above. On the other hand, registries and registrars offer customer service/support and can provide the supporting infrastructure for reliable DNS and RDAP service.

Another approach could be to handle DRIP registrations in a comparable way to how IP address space gets provisioned. Here, blocks of addresses get delegated to a "trusted" third party, typically an ISP, who then issues IP addresses to its customers. For DRIP, blocks of IP addresses could be delegated from the 3.0.0.1.0.0.2.ip6.arpa. domain (reverse domain of prefix allocated by [RFC9374]) to an entity chosen by the appropriate Civil Aviation Authority (CAA). This third party would be responsible for the corresponding DNS and RDAP infrastructure for these IP address blocks. They would also provision the Hierarchical Host Identity Tag (HHIT, [RFC9374]) records for these IP addresses. In principle a manufacturer or vendor of UAS devices could provide that role. This is shown as an example in Figure 3.

Dynamic DRIP registration is another possible solution, for example when the operator of a UAS device registers its corresponding HHIT record and other resources before a flight and deletes them afterwards. This may be feasible in controlled environments with well-behaved actors. However, this approach may not scale since each device is likely to need credentials for updating the IT infrastructure which provisions the DNS.

Registration policies (pricing, renewals, registrar and registrant agreements, etc.) will need to be developed. These considerations should be determined by the CAA, perhaps in consultation with local stakeholders to assess the cost-benefits of these approaches (and others). All of these are out of scope for this document. The specifics for the UAS RID use case are detailed in the rest of document.

4. Public Information Registry

Per [RFC9434] all information classified as public is stored in the DNS, specifically Authoritative Name Servers, to satisfy REG-1 from [RFC9153].

Authoritative Name Servers use domain names as identifiers and data is stored in Resource Records (RR) with associated RRTypes. This document defines two new RRTypes, one for HHIT metadata (HHIT, Section 5.1) and another for UAS Broadcast RID information (BRID, Section 5.2). The former RRType is particularly important as it contains a URI (as part of the certificate) that points to Private Information resources.

DETs, being IPv6 addresses, are to be under ip6.arpa. (nibble reversed per Section 2.5 of [STD88]) and MUST resolve to an HHIT RRType. Depending on local circumstances or additional use cases other RRTypes MAY be present (for example the inclusion of the DS

RRTypes or equivalent when using DNSSEC). For UAS RID the BRID RRType MUST be present to provide the Broadcast Endorsements (BEs) defined in Section 3.1.2.1 of [RFC9575].

DNSSEC MUST be used for apex entities (those which use a self-signed Canonical Registration Certificate) and is RECOMMENDED for other entities. When a DIME decides to use DNSSEC they SHOULD define a framework for cryptographic algorithms and key management [RFC6841]. This may be influenced by frequency of updates, size of the zone, and policies.

UAS-specific information, such as physical characteristics, may also be stored in DNS but is out of scope for this document.

A DET IPv6 address gets mapped into domain names using the scheme defined in Section 2.5 of [STD88]. However DNS lookups of these names query for HHIT and/or BRID resource records rather than the PTR resource records conventionally used in reverse lookups of IP addresses. For example, the HHIT resource record for the DET 2001:30::1 would be returned from a DNS lookup for the HHIT QTYPE for 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.1.0.0.2.ip6.arpa..

The HHIT RRType provides the public key for signature verification and URIs via the certificate. The BRID RRType provides static Broadcast RID information such as the Broadcast Endorsements sent following [RFC9575].

5. Resource Records

5.1. HHIT Resource Record

The HHIT Resource Record (HHIT, RRType 67) is a metadata record for various bits of HHIT-specific information that isn’t available in the pre-existing HIP RRType. The HHIT RRType does not replace the HIP RRType. The primary advantage of the HHIT RRType over the existing RRType is the mandatory inclusion of the Canonical Registration Certificate containing an entity’s public key signed by the registrar, or other trust anchor, to confirm registration.

The data MUST be encoded in CBOR [RFC8949] bytes. The CDDL [RFC8610] of the data is provided in Figure 4.

5.1.1. Text Representation

The data are represented in base64 [RFC4648] and may be divided into any number of white-space-separated substrings, down to single base64 digits, which are concatenated to obtain the full object. These substrings can span lines using the standard parenthesis. Note that the data has internal subfields but these do not appear in the master file representation; only a single logical base64 string will appear.

5.1.1.1. Presentation Representation

The data MAY, for display purposes only, be represented using the Extended Diagnostic Notation as defined in Appendix G of [RFC8610].

5.1.2. Field Descriptions

```
hhit-rr = [
    hhit-entity-type: uint,
    hid-abbreviation: tstr .size(15),
    canonical-registration-cert: bstr
]
```

Figure 4: HHIT Wire Format CDDL

All fields of the HHIT RRType MUST be included to be properly formed.

HHIT Entity Type: The HHIT Entity Type field is a number with values defined in Section 6.2.2. It is envisioned that there may be many types of HHITs in use. In some cases, it may be helpful to understand the HHITs role in the ecosystem like described in [drip-dki]. This field provides such context. This field MAY provide a signal of additional information and/or different handling of the data beyond what is defined in this document.

HID Abbreviation: The HID Abbreviation field is a string that provides an abbreviation to the HID structure of a DET for display devices. The convention for such abbreviations is a matter of local policy. Absent of such a policy, this field MUST be filled with the four character hexadecimal representations of the RAA and HDA (in that order) with a separator character such as a space. For example, a DET with an RAA value of 10 and HDA value of 20 would be abbreviated as: 000A 0014.

Canonical Registration Certificate: The Canonical Registration Certificate field is for a certificate endorsing registration of the DET. It MUST be encoded as X.509 DER [RFC5280]. This certificate MAY be self-signed when the entity is acting as a root of trust (i.e., an apex). Such self-signed behavior is defined by

policy, such as in [drip-dki], and is out of scope for this document. This certificate is part of chain of certificates that can be used to validate inclusion in the heirarchy.

5.2. UAS Broadcast RID Resource Record

The UAS Broadcast RID Resource Record (BRID, RRType 68) is a format to hold public information typically sent over UAS Broadcast RID that is static. It can act as a data source if information is not received over Broadcast RID or for cross validation. The primary function for DRIP is the inclusion of one or more Broadcast Endorsements as defined in [RFC9575] in the auth field. These Endorsements are generated by the registrar upon successful registration and broadcast by the entity.

The data MUST be encoded in CBOR [RFC8949] bytes. The CDDL [RFC8610] of the data is provided in Figure 5.

5.2.1. Text Representation

The data are represented in base64 [RFC4648] and may be divided into any number of white-space-separated substrings, down to single base64 digits, which are concatenated to obtain the full object. These substrings can span lines using the standard parenthesis. Note that the data has internal subfields but these do not appear in the master file representation; only a single logical base64 string will appear.

5.2.1.1. Presentation Representation

The data MAY, for display purposes only, be represented using the Extended Diagnostic Notation as defined in Appendix G of [RFC8610]. All byte strings longer than a length of 20 SHOULD be displayed as base64 when possible.

5.2.2. Field Descriptions

```
   bcast-rr = {
       uas_type => nibble-field,
       uas_ids => [+ uas-id-grp],
       ? auth => [+ auth-grp],
       ? self_id => self-grp,
       ? area => area-grp,
       ? classification => classification-grp,
       ? operator_id => operator-grp
   }
   uas-id-grp = [
       id_type: &uas-id-types,
       uas_id: bstr .size(20)
   ]
   auth-grp = [
       a_type: &auth-types,
       a_data: bstr .size(1..362)
   ]
   area-grp = [
       area_count: 1..255,
       area_radius: float,  # in decameters
       area_floor: float,   # wgs84-hae in meters
       area_ceiling: float  # wgs84-hae in meters
   ]
   classification-grp = [
       class_type: 0..8,
       class: nibble-field,
       category: nibble-field
   ]
   self-grp = [
       desc_type: 0..255,
       description: tstr .size(23)
   ]
   operator-grp = [
       operator_id_type: 0..255,
       operator_id: bstr .size(20)
   ]
   uas-id-types = (none: 0, serial: 1, session_id: 4)
   auth-types = (none: 0, specific_method: 5)
   nibble-field = 0..15
   uas_type = 0
   uas_ids = 1
   auth = 2
   self_id = 3
   area = 4
   classification = 5
   operator_id = 6
```

Figure 5: BRID Wire Format CDDL

The field names and their general typing are borrowed from the ASTM [F3411] data dictionary (Table 1 and Table 2). See that document for additional context and background information on aviation application-specific interpretation of the field semantics. The explicitly enumerated values included in the CDDL above are relevant to DRIP for its operation. Other values may be valid but are outside the scope of DRIP operation. Application-specific fields, such as UAS Type are transported and authenticated by DRIP but are regarded as opaque user data to DRIP.

6. IANA Considerations

6.1. DET Prefix Delegation

The reverse domain for the DET Prefix, i.e., 3.0.0.1.0.0.2.ip6.arpa., is managed by the IANA following the usual IANA rules. IANA will liaise, as needed, with the International Civil Aviation Organization (ICAO) to verify the authenticity of delegations to CAAs (see Section 6.2.1.4).

6.2. IANA DRIP Registry

6.2.1. DRIP RAA Allocations

This document requests a new registry for RAA Allocations under the DRIP registry group (https://www.iana.org/assignments/drip) to be managed by IANA.

RAA Allocations: a 14-bit value used to represent RAAs. Future additions to this registry are to be made based on the following range/policy table:

RAA Range	Allocation	Policy
0 - 3	Reserved	N/A
4 - 3999	ISO 3166-1 Countries	IESG Approval (Section 4.10 of [RFC8126]), Section 6.2.1.4
4000 - 8191	Reserved	N/A
8192 - 15359	Unassigned	First Come First Served (Section 4.4 of [RFC8126])
15360 - 16383	Private Use	Private Use (Section 4.1 of [RFC8126]), Section 6.2.1.5

Table 1: RAA Ranges

6.2.1.1. RAA Allocation Fields

Value: The RAA value delegated for this entry.

Name: Name of the delegated RAA. For the ISO 3166-1 Countries (Section 6.2.1.4), this should be the name of the country.

Policy Reference: A publicly accessible link to the requirements for prospective HDA operators to register under this RAA. This field is OPTIONAL.

Contact: Contact details of the administrator of this RAA that prospective HDAs operators can make informational queries to.

6.2.1.2. RAA Registration Form

```
Value:
Name:
Policy Reference:
Contact:
NS RRType Content (HDA=0):
NS RRType Content (HDA=4096):
NS RRType Content (HDA=8192):
NS RRType Content (HDA=12288):
```

Figure 6: RAA Delegation Request Form

The NS RRType Content (HDA=X) fields are used by IANA to perform the DNS delegations under 3.0.0.1.0.0.2.ip6.arpa.. See Section 6.2.1.3 for technical details.

6.2.1.3. Handling Nibble Split

To support DNS delegation in 3.0.0.1.0.0.2.ip6.arpa. a single RAA is given 4 delegations by borrowing the upper two bits of HDA space (see Figure 7 for an example). This enables a clean nibble boundary in DNS to delegate from (i.e., the prefix 2001:3x:xxx0::/44). These HDAs (0, 4096, 8192 and 12288) are reserved for the RAA.

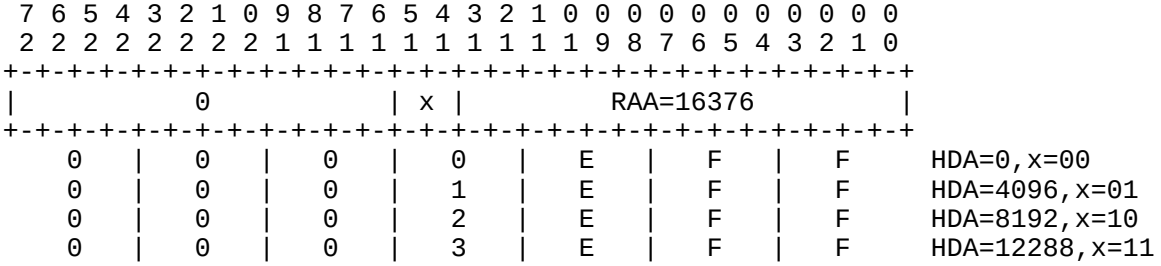


Figure 7: Example Bit Borrowing of RAA=16376

6.2.1.4. ISO 3166-1 Countries Range

The mapping between ISO 3166-1 Numeric Nation Codes and RAAs is specified and documented by IANA. Each Nation is assigned four RAAs that are left to the national authority for their purpose. For RAAs under this range, a shorter prefix of 2001:3x:xx00::/40 MAY be delegated to each CAA, which covers all 4 RAAs (and reserved HDAs) assigned to them.

This range is set to IESG Approval (Section 4.10 of [RFC8126]) and IANA will liaise with the ICAO to verify the authenticity of delegation requests (using Figure 6) by CAAs.

> The CSV file found for the ISO to RAA mapping is on GitHub (https://github.com/ietf-wg-drip/draft-ietf-drip-registries/commit/a8da51bfcafcdf91878f8862c52830aa736782c9). RFC Editor, please remove this note after IANA initializes the registry but before publication.

6.2.1.5. Private Range

If nibble-reversed lookup in DNS is desired it can only provided by private DNS servers as zone delegations from the global root will not be performed for this address range. Thus the RAAs (with its subordinate HDAs) in this range may be used in like manner and IANA will not delegate any value in this range to any party (as per Private Use, Section 4.1 of [RFC8126]).

One anticipated acceptable use of the private range is for experimentation and testing prior to request allocation or assignment from IANA.

6.2.2. HHIT Entity Type

This document requests a new registry for HHIT Entity Type under the DRIP registry group (https://www.iana.org/assignments/drip).

HHIT Entity Type: numeric, field of the HHIT RRType to encode the HHIT Entity Type. All entries in this registry are under a First Come First Served (Section 4.4 of [RFC8126]) policy.

6.2.2.1. HHIT Type Registry Fields

Value: HHIT Type value of entry.

HHIT Type: Name of the entry and optional abbreviation.

Reference: Public document allocating the value and any additional information such as semantics. This can be a URL pointing to an Internet-Draft, IETF RFC, or web-page among others.

6.2.2.2. HHIT Type Registration Form

Value:
HHIT Type:
Reference:

Figure 8: HHIT Type Registration Form

6.2.2.3. Initial Values

The following values are defined by this document:

Value	HHIT Type	Reference
0	Not Defined	This RFC
1	DRIP Identity Management Entity (DIME)	This RFC
5	Apex	This RFC
9	Registered Assigning Authority (RAA)	This RFC
13	HHIT Domain Authority (HDA)	This RFC
16	Unmanned Aircraft (UA)	This RFC
17	Ground Control Station (GCS)	This RFC
18	Unmanned Aircraft System (UAS)	This RFC
19	Remote Identification (RID) Module	This RFC
20	Pilot	This RFC
21	Operator	This RFC
22	Discovery & Synchronization Service (DSS)	This RFC
23	UAS Service Supplier (USS)	This RFC
24	Network RID Service Provider (SP)	This RFC
25	Network RID Display Provider (DP)	This RFC
26	Supplemental Data Service Provider (SDSP)	This RFC
27	Crowd Sourced RID Finder	This RFC

Table 2: HHIT Entity Type Initial Values

7. Security Considerations

7.1. DNS Operational & Registration Considerations

The Registrar and Registry are commonly used concepts in the DNS. These components interface the DIME into the DNS hierarchy and thus operation SHOULD follow best common practices, specifically in security (such as running DNSSEC) as appropriate except when national regulations prevent it. [BCP237] provides suitable guidance.

If DNSSEC is used, a DNSSEC Practice Statement SHOULD be developed and published. It SHOULD explain how DNSSEC has been deployed and what security measures are in place. [RFC6841] documents a Framework for DNSSEC Policies and DNSSEC Practice Statements. A self-signed entity (i.e. an entity that self-signed it certificate as part of the HHIT RRType) MUST use DNSSEC.

The interfaces and protocol specifications for registry-registrar interactions are intentionally not specified in this document. These will depend on nationally defined policy and prevailing local circumstances. It is expected registry-registrar activity will use the Extensible Provisioning Protocol (EPP) [STD69] or equivalent. The registry SHOULD provide a lookup service such as RDAP [STD95] or equivalent to publish public information about registered domain names.

Decisions about DNS or registry best practices and other operational matters that influence security SHOULD be made by the CAA, ideally in consultation with local stakeholders.

The guidance above is intended to reduce the likelihood of interoperability problems and minimize security and stability concerns. For instance, validation and authentication of DNS responses depends on DNSSEC. If this is not used, entities using DRIP will be vulnerable to DNS spoofing attacks and could be exposed to bogus data. DRIP DNS responses that have not been validated by DNSSEC could contain bogus data which have the potential to create serious security problems and operational concerns for DRIP entities. These threats include denial of service attacks, replay attacks, impersonation or cloning of UAVs, hijacking of DET registrations, injection of corrupt metadata and compromising established trust architecture/relationships. Some regulatory and legal considerations are expected to be simplified by providing a lookup service for access to public information about registered domain names for DETs.

When DNSSEC is not in use, due to the length of the ORCHID hash selected for DETs (Section 3.5 of [RFC9374]), clients MUST "walk" the tree of certificates locating each certificate by performing DNS lookups of HHIT RRTypes for each DET verifying inclusion into the hierarchy. The collection of these certificates (which provide both signature protection from the parent entity and the public key of the entity) is the only way without DNSSEC to prove valid registration.

The contents of the BRID RRType auth key, containing Endorsements as described in Section 4.2 of [RFC9575], are a shadow of the X.509 certificate found in the HHIT RRType. The validation of these Endorsements follow the guidelines written in Section 6.4.2 of [RFC9575] for Broadcast RID Observers and when present MUST also be validated.

7.2. DET & Public Key Exposure

DETs are built upon asymmetric keys. As such the public key must be revealed to enable clients to perform signature verifications. [RFC9374] security considerations cover various attacks on such keys. While unlikely, the forging of a corresponding private key is possible if given enough time (and computational power).

When practical, it is RECOMMENDED that no RRTypes under a DET’s specific domain name be published unless and until it is required for use by other parties. Such action would cause at least the HHIT RRType to not be in DNS, protecting the public key in the certificate from being exposed before its needed. The combination of this "just in time" publishing mechanism and DNSSEC is out of scope for this document.

Optimally this requires that the UAS somehow signal the DIME that a flight using a Specific Session ID will soon be underway or complete. It may also be facilitated under UTM if the USS (which may or may not be a DIME) signals when a given operation using a Session ID goes active.

8. Acknowledgements

Thanks to Stuart Card (AX Enterprize, LLC) and Bob Moskowitz (HTT Consulting, LLC) for their early work on the DRIP registries concept. Their early contributions laid the foundations for the content and processes of this architecture and document.

9. References

9.1. Normative References

[F3411] ASTM International, "Standard Specification for Remote ID and Tracking", ASTM F3411-22A, DOI 10.1520/F3411-22A, July 2022, <https://www.astm.org/f3411-22a.html>.

[ISO3166-1] International Standards Organization (ISO), "Codes for the representation of names of countries and their subdivisions", ISO 3166-1:2020, August 2020, <https://www.iso.org/iso-3166-country-codes.html>.

[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/rfc/rfc2119>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/rfc/rfc4648>.

[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/rfc/rfc8174>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/rfc/rfc9374>.

9.2. Informative References

[BCP237] Best Current Practice 237, <https://www.rfc-editor.org/info/bcp237>. At the time of writing, this BCP comprises the following:

Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[drip-dki] Moskowitz, R. and S. W. Card, "The DRIP DET public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-drip-dki-08, 22 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-drip-dki-08>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC6841] Ljunggren, F., Eklund Lowinder, AM., and T. Okubo, "A Framework for DNSSEC Policies and DNSSEC Practice Statements", RFC 6841, DOI 10.17487/RFC6841, January 2013, <https://www.rfc-editor.org/rfc/rfc6841>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC9153] Card, S., Ed., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements and Terminology", RFC 9153, DOI 10.17487/RFC9153, February 2022, <https://www.rfc-editor.org/rfc/rfc9153>.

[RFC9434] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., Ed., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", RFC 9434, DOI 10.17487/RFC9434, July 2023, <https://www.rfc-editor.org/rfc/rfc9434>.

[RFC9575] Wiethuechter, A., Ed., Card, S., and R. Moskowitz, "DRIP Entity Tag (DET) Authentication Formats and Protocols for Broadcast Remote Identification (RID)", RFC 9575, DOI 10.17487/RFC9575, June 2024, <https://www.rfc-editor.org/rfc/rfc9575>.

[STD13] Internet Standard 13, <https://www.rfc-editor.org/info/std13>. At the time of writing, this STD comprises the following:

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

Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[STD69] Internet Standard 69, <https://www.rfc-editor.org/info/std69>. At the time of writing, this STD comprises the following:

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

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>.

Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Host Mapping", STD 69, RFC 5732, DOI 10.17487/RFC5732, August 2009, <https://www.rfc-editor.org/info/rfc5732>.

Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Contact Mapping", STD 69, RFC 5733, DOI 10.17487/RFC5733, August 2009, <https://www.rfc-editor.org/info/rfc5733>.

Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport over TCP", STD 69, RFC 5734, DOI 10.17487/RFC5734, August 2009, <https://www.rfc-editor.org/info/rfc5734>.

[STD88] Internet Standard 88, <https://www.rfc-editor.org/info/std88>. At the time of writing, this STD comprises the following:

Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003, <https://www.rfc-editor.org/info/rfc3596>.

[STD95] Internet Standard 95, <https://www.rfc-editor.org/info/std95>. At the time of writing, this STD comprises the following:

Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/info/rfc7481>.

Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

Blanchet, M., "Finding the Authoritative Registration Data Access Protocol (RDAP) Service", STD 95, RFC 9224, DOI 10.17487/RFC9224, March 2022, <https://www.rfc-editor.org/info/rfc9224>.

Appendix A. Example Zone Files & RRType Contents

An example zone file ip6.arpa., run by IANA, is not shown. It would contain NS RRTypes to delegate to a respective RAA. To avoid any future collisions with production deployments an apex of ip6.example.com. is used instead of ip6.arpa.. All hexadecimal strings in the examples are broken into the lengths of a word, for document formatting purposes.

An RAA with a HID of RAA=16376, HDA=0 and HDA with a the HID RAA=16376, HDA=10 were used in the examples.

A.1. Example RAA

A.1.1. Authentication HHIT

```
$ORIGIN 5.0.0.0.0.0.e.f.f.3.0.0.1.0.0.2.ip6.example.com.
7.b.0.a.1.9.e.1.7.5.1.a.0.6.e.5. IN HHIT (
    gwppM2ZmOCAwMDAwWQFGMIIBQjCB9aAD
    AgECAgE1MAUGAytlcDArMSkwJwYDVQQD
    DCAyMDAxMDAzZmZlMDAwMDA1NWU2MGEx
    NTcxZTkxYTBiNzAeFw0yNTA0MDkyMDU2
    MjZaFw0yNTA0MDkyMTU2MjZaMB0xGzAZ
    BgNVBAMMEkRSSVAtUkFBLUEtMTYzNzYt
    MDAqMAUGAytlcAMhAJmQ1bBLcqGAZtQJ
    K1LH1JlPt8Fr1+jB9ED/qNBP8eE/o0ww
    SjAPBgNVHRMBAf8EBTADAQH/MDcGA1Ud
    EQEB/wQtMCuHECABAD/+AAAFXmChVx6R
    oLeGF2h0dHBzOi8vcmFhLmV4YW1wbGUu
    Y29tMAUGAytlcANBALUPjhIB3rwqXQep
    r9/VDB+hhtwuWZIw1OUkEuDrF6DCkgc7
    5widXnXa5/uDfdKL7dZ83mPHm2Tf32Dv
    b8AzEw8=
)
```

Figure 9: RAA Auth HHIT RRType Example

Figure 10 shows the CBOR decoded RDATA in the HHIT RRType found in Figure 9.

```
[
    10,  # Reserved (RAA Auth from DKI)
    "3ff8 0000",
    h'308201423081F5A00302010202013530
    0506032B6570302B312930270603550403
    0C20323030313030336666653030303030
    353565363061313537316539316130623 7
    301E170D3235303430393230353632365A
    170D3235303430393231353632365A301D
    311B301906035504030C12445249502D52
    41412D412D31363337362D30302A300506
    032B65700321009990D5B04B72A18066D4
    092B52C7D4994FB7C16BD7E8C1F440FFA8
    D04FF1E13FA34C304A300F0603551D1301
    01FF040530030101FF30370603551D1101
    01FF042D302B87102001003FFE0000055E
    60A1571E91A0B7861768747470733A2F2F
    7261612E6578616D706C652E636F6D3005
    06032B6570034100B50F8E1201DEBC2A5D
    07A9AFDFD50C1FA186DC2E599230D4E524
    12E0EB17A0C292073BE7089D5E75DAE7FB
    837DD28BEDD67CDE63C79B64DFDF60EF6F
    C033130F'
]
```

Figure 10: 2001:3f:fe00:5:5e60:a157:1e91:a0b7 Decoded HHIT RRType CBOR

Figure 11 shows the decoded DER X.509 found in Figure 10.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 53 (0x35)
        Signature Algorithm: ED25519
        Issuer: CN = 2001003ffe0000055e60a1571e91a0b7
        Validity
            Not Before: Apr  9 20:56:26 2025 GMT
            Not After : Apr  9 21:56:26 2025 GMT
        Subject: CN = DRIP-RAA-A-16376-0
        Subject Public Key Info:
            Public Key Algorithm: ED25519
                ED25519 Public-Key:
                pub:
                    99:90:d5:b0:4b:72:a1:80:66:d4:09:2b:52:c7:d4:
                    99:4f:b7:c1:6b:d7:e8:c1:f4:40:ff:a8:d0:4f:f1:
                    e1:3f
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Alternative Name: critical
                IP Address:2001:3F:FE00:5:5E60:A157:1E91:A0B7,
                URI:https://raa.example.com
    Signature Algorithm: ED25519
    Signature Value:
        b5:0f:8e:12:01:de:bc:2a:5d:07:a9:af:df:d5:0c:1f:a1:86:
        dc:2e:59:92:30:d4:e5:24:12:e0:eb:17:a0:c2:92:07:3b:e7:
        08:9d:5e:75:da:e7:fb:83:7d:d2:8b:ed:d6:7c:de:63:c7:9b:
        64:df:df:60:ef:6f:c0:33:13:0f
```

Figure 11: 2001:3f:fe00:5:5e60:a157:1e91:a0b7 Decoded Certificate

A.1.2. Delegation of HDA

```
$ORIGIN c.d.f.f.3.0.0.1.0.0.2.ip6.example.com.
a.0.0. IN NS ns1.hda-10.example.com
```

Figure 12: HDA Delegation Example

A.2. Example HDA

A.2.1. Authentication & Issue HHITs

```
$ORIGIN 5.0.a.0.0.0.e.f.f.3.0.0.1.0.0.2.ip6.example.com.
0.a.9.0.7.2.4.d.5.4.e.e.5.1.6.6.5.0. IN HHIT (
    gw5pM2ZmOCAwMDBhWQFHMIIBQzCB9qAD
    AgECAgFfMAUGAytlcDArMSkwJwYDVQQD
    DCAyMDAxMDAzZmZlMDAwMDA1NWU2MGEx
    NTcxZTkxYTBiNzAeFw0yNTA0MDkyMTAz
    MTlaFw0yNTA0MDkyMjAzMTlaMB4xHDAa
    BgNVBAMME0RSSVAtSERBLUEtMTYzNzYt
    MTAwKjAFBgMrZXADIQDOaB424RQa61YN
    bna8eWt7fLRU5GPMsfEt4wo4AQGAP6NM
    MEowDwYDVR0TAQH/BAUwAwEB/zA3BgNV
    HREBAf8ELTArhxAgAQA//gAKBWYV7kXU
    JwmghhdodHRwczovL3JhYS5leGFtcGxl
    LmNvbTAFBgMrZXADQQAhMpOSOmgMkJY1
    f+B9nTgawUjK4YEERBtczMknHDkOowX0
    ynbaLN60TYe9hqN6+CJ3SN8brJke3hpM
    gorvhDkJ
)
8.2.e.6.5.2.b.6.7.3.4.d.e.0.6.2.5.0. IN HHIT (
    gw9pM2ZmOCAwMDBhWQFHMIIBQzCB9qAD
    AgECAgFYMAUGAytlcDArMSkwJwYDVQQD
    DCAyMDAxMDAzZmZlMDAwYTA1NjYxNWVl
    NDVkNDI3MDlhMDAeFw0yNTA0MDkyMTA1
    MTRaFw0yNTA0MDkyMjA1MTRaMB4xHDAa
    BgNVBAMME0RSSVAtSERBLUktMTYzNzYt
    MTAwKjAFBgMrZXADIQCCM/2utQaLwUhZ
    0ROg7fz43AeBTj3Sdl5rW4LgTQcFl6NM
    MEowDwYDVR0TAQH/BAUwAwEB/zA3BgNV
    HREBAf8ELTArhxAgAQA//gAKBSYO1Ddr
    JW4ohhdodHRwczovL2hkYS5leGFtcGxl
    LmNvbTAFBgMrZXADQQBa8lZyftxHJqDF
    Vgv4Rt+cMUmc8aQwet4UZdO3yQOB9uq4
    sLVAScaZCWjC0nmeRkgVRhize1esfyi3
    RRU44IAE
)
```

Figure 13: HDA Auth/Issue HHIT RRType Example

Figure 14 shows the CBOR decoded RDATA in the HHIT RRType found in Figure 13.

```
[
    14,  # Reserved (HDA Auth from DKI)
    "3ff8 000a",
    h'308201433081F6A00302010202015F30
    0506032B6570302B312930270603550403
    0C2032303031303033666665303030303030
    3535653630613135373165393161306237
    301E170D3235303430393231303331395A
    170D3235303430393232303331395A301E
    311C301A06035504030C13445249502D48
    44412D412D31363337362D3130302A3005
    06032B6570032100CE681E36E1141AEB56
    0D6E76BC796B7B7CB454E463CCB1F12DE3
    0A380101803FA34C304A300F0603551D13
    0101FF040530030101FF30370603551D11
    0101FF042D302B87102001003FFE000A05
    6615EE45D42709A0861768747470733A2F
    2F7261612E6578616D706C652E636F6D30
    0506032B6570034100213293923A680C90
    96357FE07D9D381AC148CAE18104441B5C
    CCC9271C390EA305F4CA76DA2CDEB44D87
    BD86A37AF8227748DF1BAC991EDE1A4C82
    8AEF843909'
]
```

Figure 14: 2001:3f:fe00:a05:6615:ee45:d427:9a0 Decoded HHIT RRType CBOR

Figure 15 shows the decoded DER X.509 found in Figure 14.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 95 (0x5f)
        Signature Algorithm: ED25519
        Issuer: CN = 2001003ffe0000055e60a1571e91a0b7
        Validity
            Not Before: Apr  9 21:03:19 2025 GMT
            Not After : Apr  9 22:03:19 2025 GMT
        Subject: CN = DRIP-HDA-A-16376-10
        Subject Public Key Info:
            Public Key Algorithm: ED25519
                ED25519 Public-Key:
                pub:
                    ce:68:1e:36:e1:14:1a:eb:56:0d:6e:76:bc:79:6b:
                    7b:7c:b4:54:e4:63:cc:b1:f1:2d:e3:0a:38:01:01:
                    80:3f
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Alternative Name: critical
                IP Address:2001:3F:FE00:A05:6615:EE45:D427:9A0,
                URI:https://raa.example.com
    Signature Algorithm: ED25519
    Signature Value:
        21:32:93:92:3a:68:0c:90:96:35:7f:e0:7d:9d:38:1a:c1:48:
        ca:e1:81:04:44:1b:5c:cc:c9:27:1c:39:0e:a3:05:f4:ca:76:
        da:2c:de:b4:4d:87:bd:86:a3:7a:f8:22:77:48:df:1b:ac:99:
        1e:de:1a:4c:82:8a:ef:84:39:09
```

Figure 15: 2001:3f:fe00:a05:6615:ee45:d427:9a0 Decoded Certificate

Figure 16 shows the CBOR decoded RDATA in the HHIT RRType found in Figure 13.

```
[
    15,  # Reserved (HDA Issue from DKI)
    "3ff8 000a",
    h'308201433081F6A00302010202015830
    0506032B6570302B312930270603550403
    0C2032303031303033666665303030306130
    3536363135656534356434323730396130
    301E170D3235303430393231303531345A
    170D3235303430393232303531345A301E
    311C301A06035504030C13445249502D48
    44412D492D31363337362D3130302A3005
    06032B6570321008233FDAEB5068BC148
    59D113A0EDFCF8DC07814E3DD2765E6B5B
    82E04D070597A34C304A300F0603551D13
    0101FF040530030101FF30370603551D11
    0101FF042D302B87102001003FFE000A05
    260ED4376B256E28861768747470733A2F
    2F6864612E6578616D706C652E636F6D30
    0506032B65700341005AF256727EDC4726
    A0C5560BF846DF9C31499CF1A4307ADE14
    65D3B7C90381F6EAB8B0B54049C6990968
    C2D2799E4648154618B37B57AC7F28B745
    1538E08004'
]
```

Figure 16: 2001:3f:fe00:a05:260e:d437:6b25:6e28 Decoded HHIT RRType CBOR

Figure 17 shows the decoded DER X.509 found in Figure 16.

```
   Certificate:
       Data:
           Version: 3 (0x2)
           Serial Number: 88 (0x58)
           Signature Algorithm: ED25519
           Issuer: CN = 2001003ffe000a056615ee45d42709a0
           Validity
               Not Before: Apr  9 21:05:14 2025 GMT
               Not After : Apr  9 22:05:14 2025 GMT
           Subject: CN = DRIP-HDA-I-16376-10
           Subject Public Key Info:
               Public Key Algorithm: ED25519
                   ED25519 Public-Key:
                   pub:
                       82:33:fd:ae:b5:06:8b:c1:48:59:d1:13:a0:ed:fc:
                       f8:dc:07:81:4e:3d:d2:76:5e:6b:5b:82:e0:4d:07:
                       05:97
           X509v3 extensions:
               X509v3 Basic Constraints: critical
                   CA:TRUE
               X509v3 Subject Alternative Name: critical
                   IP Address:2001:3F:FE00:A05:260E:D437:6B25:6E28,
                   URI:https://hda.example.com
       Signature Algorithm: ED25519
       Signature Value:
           5a:f2:56:72:7e:dc:47:26:a0:c5:56:0b:f8:46:df:9c:31:49:
           9c:f1:a4:30:7a:de:14:65:d3:b7:c9:03:81:f6:ea:b8:b0:b5:
           40:49:c6:99:09:68:c2:d2:79:9e:46:48:15:46:18:b3:7b:57:
           ac:7f:28:b7:45:15:38:e0:80:04
```

Figure 17: 2001:3f:fe00:a05:260e:d437:6b25:6e28 Decoded Certificate

A.2.2. Registratant HHIT & BRID

```
$ORIGIN 5.0.a.0.0.0.e.f.f.3.0.0.1.0.0.2.ip6.example.com.
2.b.6.c.b.4.a.9.9.6.4.2.8.0.3.1. IN HHIT (
    gxJpM2ZmOCAwMDBhWQEYMIIBFDCBx6AD
    AgECAgFUMAUGAytlcDArMSkwJwYDVQQD
    DCAyMDAxMDAzZmZlMDAwYTA1MjYwZWQ0
    Mzc2YjI1NmUyODAeFw0yNTA0MDkyMTEz
    MDBaFw0yNTA0MDkyMjEzMDBaMAAwKjAF
    BgMrZXADIQDJLi+dl+iWD5tfFlT4sJA5
    +drcW88GHqxPDOp56Oh3+qM7MDkwNwYD
    VR0RAQH/BC0wK4cQIAEAP/4ACgUTCCRp
    mkvGsoYXaHR0cHM6Ly9oZGEuZXhhbXBs
    ZS5jb20wBQYDK2VwA0EA0DbcdngC7/BB
    /aLjZmLieo0ZFCDbd/KIxAy+3X2KtT4J
    todVxRMPAkN6o008gacbNfTG8p9npEcD
    eYhesl2jBQ==
)
2.b.6.c.b.4.a.9.9.6.4.2.8.0.3.1. IN BRID (
    owAAAYIEUQEgAQA//gAKBRMIJGmaS8ay
    AogFWIkB+t72Zwrt9mcgAQA//gAABV5g
    oVcekaC3mZDVsEtyoYBm1AkrUsfUmU+3
    wWvX6MH0QP+o0E/x4T8gAQA//gAABV5g
    oVcekaC3vC9m1JguvXt7W2o4wxPumaT1
    IP3TQN3fQP28hpInSIlsSwq8UCNjm2ad
    7pdTvm2EqfOJQNPKClvRZm4qTO5FDAVY
    iQGX4PZnp+72ZyABAD/+AAoFZhXuRdQn
    CaDOaB424RQa61YNbna8eWt7fLRU5GPM
    sfEt4wo4AQGAPyABAD/+AAAFXmChVx6R
    oLfv3q+mLRB3ya5TmjY8+3CzdoDZT9RZ
    +XpN5hDiA6JyyxBJvUewxLzPNhTXQp8v
    ED71XAE82tMmt3fB4zbzWNQLBViJAQrh
    9mca7/ZnIAEAP/4ACgUmDtQ3ayVuKIIz
    /a61BovBSFnRE6Dt/PjcB4FOPdJ2Xmtb
    guBNBwWXIAEAP/4ACgVmFe5F1CcJoIjy
    CriJCxAyAWTOHPmlHL02MKSpsHviiTze
    qwBH9K/Rrz41CYix9HazAIOAZO8FcfU5
    M+WLLJZoaQWBHnMbTQwFWIkB3OL2Z+zw
    9mcgAQA//gAKBRMIJGmaS8ayyS4vnZfo
    lg+bXxZU+LCQOfna3FvPBh6sTwzqeejo
    d/ogAQA//gAKBSYO1DdrJW4ogOfc8jTi
    mYLmTOOyFZoUx2jOOwtB1jnqUJr6bYaw
    MoPrR3MlKGBGWsVz1yXNqUURoCqYdwsY
    e61vd5i6YJqnAQ==
)
```

Figure 18: Registrant HHIT/BRID RRType Example

Figure 19 shows the CBOR decoded RDATA in the HHIT RRType found in Figure 18.

```
[
    18,  # Uncrewed Aircraft System (UAS)
    "3ff8 000a",
    h'308201143081C7A00302010202015430
    0506032B6570302B312930270603550403
    0C20323030313030336666653030306130
    353236306564343337366232353665323 8
    301E170D3235303430393231313330305A
    170D3235303430393232313330305A3000
    302A300506032B6570032100C92E2F9D97
    E8960F9B5F1654F8B09039F9DADC5BCF06
    1EAC4F0CEA79E8E877FAA33B3039303706
    03551D110101FF042D302B87102001003F
    FE000A05130824699A4BC6B28617687474
    70733A2F2F6864612E6578616D706C652E
    636F6D300506032B6570034100D036DC76
    7802EFF041FDA2E36662E27A8D191420DB
    77F288C40CBEDD7D8AB53E09B68755C513
    0F02437AA34D3C81A71B35F4C6F29F67A4
    470379885EB25DA305'
]
```

Figure 19: 2001:3f:fe00:a05:1308:2469:9a4b:c6b2 Decoded HHIT RRType CBOR

Figure 20 shows the decoded DER X.509 found in Figure 19.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 84 (0x54)
        Signature Algorithm: ED25519
        Issuer: CN = 2001003ffe000a05260ed4376b256e28
        Validity
            Not Before: Apr  9 21:13:00 2025 GMT
            Not After : Apr  9 22:13:00 2025 GMT
        Subject:
        Subject Public Key Info:
            Public Key Algorithm: ED25519
                ED25519 Public-Key:
                pub:
                    c9:2e:2f:9d:97:e8:96:0f:9b:5f:16:54:f8:b0:90:
                    39:f9:da:dc:5b:cf:06:1e:ac:4f:0c:ea:79:e8:e8:
                    77:fa
        X509v3 extensions:
            X509v3 Subject Alternative Name: critical
                IP Address:2001:3F:FE00:A05:1308:2469:9A4B:C6B2,
                URI:https://hda.example.com
    Signature Algorithm: ED25519
    Signature Value:
        d0:36:dc:76:78:02:ef:f0:41:fd:a2:e3:66:62:e2:7a:8d:19:
        14:20:db:77:f2:88:c4:0c:be:dd:7d:8a:b5:3e:09:b6:87:55:
        c5:13:0f:02:43:7a:a3:4d:3c:81:a7:1b:35:f4:c6:f2:9f:67:
        a4:47:03:79:88:5e:b2:5d:a3:05
```

Figure 20: 2001:3f:fe00:a05:1308:2469:9a4b:c6b2 Decoded Certificate

Figure 21 shows the CBOR decoded RDATA of the BRID RRType in Figure 18.

```
{
    0: 0,
    1: [4, h'012001003FFE000A05130824699A4BC6B2'],
    2: [
        5,
        h'01FADEF6670AEDF6672001003FFE0000
        055E60A1571E91A0B79990D5B04B72A180
        66D4092B52C7D4994FB7C16BD7E8C1F440
        FFA8D04FF1E13F2001003FFE0000055E60
        A1571E91A0B7BC2F66D4982EBD7B7B5B6A
        38C313EE99A4F520FDD340DDDF40FDBC86
        922748896C4B0ABC5023639B669DEE9753
        BE6D84A9F38940D3CA0A5BD1666E2A4CEE
        450C',
        5,
        h'0197E0F667A7EEF6672001003FFE000A
        056615EE45D42709A0CE681E36E1141AEB
        560D6E76BC796B7B7CB454E463CCB1F12D
        E30A380101803F2001003FFE0000055E60
        A1571E91A0B7EFDEAFA62D1077C9AE539A
        363CFB70B37680D94FD459F97A4DE610E2
        03A272CB1049BD47B0C4BCCF3614D7429F
        2F103EF55C013CDAD326B777C1E336F358
        D40B',
        5,
        h'010AE1F6671AEFF6672001003FFE000A
        05260ED4376B256E288233FDAEB5068BC1
        4859D113A0EDFCF8DC07814E3DD2765E6B
        5B82E04D0705972001003FFE000A056615
        EE45D42709A088F20AB8890B10320164CE
        1CF9A51CBD3630A4A9B07BE2893CDEAB00
        47F4AFD1AF3E350988B1F476B300838064
        EF0571F53933E58B2C96686905811E731B
        4D0C',
        5,
        h'01DCE2F667ECF0F6672001003FFE000A
        05130824699A4BC6B2C92E2F9D97E8960F
        9B5F1654F8B09039F9DADC5BCF061EAC4F
        0CEA79E8E877FA2001003FFE000A05260E
        D4376B256E2880E7DCF234E29982E64CE3
        B2159A14C768CE3B0B41D639EA509AFA6D
        86B03283EB4773252860465AC573D725CD
        A94511A02A98770B187BAD6F7798BA609A
        A701'
    ]
}
```

Figure 21: 2001:3f:fe00:a05:1308:2469:9a4b:c6b2 Decoded BRID RRType CBOR

Authors' Addresses

Adam Wiethuechter (editor)
AX Enterprize, LLC
4947 Commercial Drive
Yorkville, NY 13495
United States of America
Email: adam.wiethuechter@axenterprize.com

Jim Reid
RTFM llp
St Andrews House
382 Hillington Road, Glasgow Scotland
G51 4BL
United Kingdom
Email: jim@rfc1035.com