Authors: A. Wiethuechter   S. Card
          AX Enterprize, LLC   AX Enterprize, LLC
          R. Moskowitz
          HTT Consulting

DRIP Provisioning Agent (DPA) Client HTTP Interface

Abstract

   This document defines an HTTP based interface using either JSON or
   CBOR for object encodings for clients to register in a DRIP Identity
   Management Entity (DIME). The DPA is a logical component of the DIME
   that handles various DRIP specific functions and is the public
   interface for clients that wish to register.

Status of This Memo

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

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

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

   This Internet-Draft will expire on 31 March 2023.

Copyright Notice

Table of Contents

1. Introduction

The DPA is one of the required components in a DIME for it to
fulfill the role of registration of DRIP Entity Tags (DETs) of
clients. A standardized interface is needed for this to avoid
interoperability issues between vendors supporting DRIP and the
various logical components of the DIME.

Per [drip-detim] the DPA MUST:

   provided an HTTP interface for clients to access with JSON or
   CBOR encoding of objects being sent to the DPA.

This document is the definition of this interface and its behavior;
specifically between the DPA and a registering client. A snapshot of
the OpenAPI specification is in [Appendix A]() at the time of this
documents publishing; with a URI to access an updated specification.

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.

3. Endpoint Definitions & Behavior

All endpoints that send DRIP Endorsements use the JSON/CBOR forms as specified in [drip-detim].

If there is any failure during validation in any endpoint a HTTP 400 code MUST be sent to the client with a detailed reason for the error.

3.1. Serial Number

3.1.1. Standard Serial Number

```
{
    "serial": "Serial Number",
    "metadata": {
        "manufacturer": "Manufacturer",
        "make": "Make",
        "model": "Model",
        "color": "Color",
        "material": "Material",
        "weight": 1.0,
        "length": 1.0,
        "width": 1.0,
        "height": 1.0,
        "numRotors": 1,
        "propLength": 1.0,
        "batteryCapacity": 1.0,
        "batteryVoltage": 1.0,
        "batteryWeight": 1.0,
        "batteryChemistry": "Battery Chemistry",
        "takeOffWeight": 1.0,
        "maxPayloadWeight": 0.1,
        "maxFlightTime": 1.0,
        "minOperatingTemp": 1.0,
        "maxOperatingTemp": 2.0,
        "ipRating": "None"
    }
}
```

When a Serial Number request comes in the Serial Number MUST be validated to the formatting specified in [CTA2063A]}. If the Serial Number is valid the DPA MUST check to confirm that there is no collisions are present for the Serial Number in both the Registry/ Name Server (using the Serial Number FQDN) and the DIA.

If no collisions are detected the metadata can be sent to the DIA using the Serial Number as the primary key value.

A successful registration MUST return a HTTP code 200 with the
following payload:

```
{
    "serial_fqdn": "<id>.<mfr_code>.mfr.hhit.arpa."
}
```

3.1.2. DET Serial Number

```
{
    "serial": "Serial Number",
    "se": self_endorsement,
    "metadata": {
        "manufacturer": "Manufacturer",
        "make": "Make",
        "model": "Model",
        "color": "Color",
        "material": "Material",
        "weight": 1.0,
        "length": 1.0,
        "width": 1.0,
        "height": 1.0,
        "numRotors": 1,
        "propLength": 1.0,
        "batteryCapacity": 1.0,
        "batteryVoltage": 1.0,
        "batteryWeight": 1.0,
        "batteryChemistry": "Battery Chemistry",
        "takeOffWeight": 1.0,
        "maxPayloadWeight": 0.1,
        "maxFlightTime": 1.0,
        "minOperatingTemp": 1.0,
        "maxOperatingTemp": 2.0,
        "ipRating": "None"
    }
}
```

The self_endorsement in the request is a Self-Endorsement: UA.

The serial parameter when using a DET-based Serial Number must be
checked to confirm that the DET in the Self-Endorsement: UA properly
encodes into the Serial Number specified. The formatting and process
of a DET encoded Serial Number can be found in [drip-rid].

If the Serial Number is valid the DPA MUST check to confirm that
there is no collisions are present for the Serial Number, DET and HI
in both the Registry/Name Server (using the DET FQDN and Serial
Number FQDN) and the DIA.

If no collisions are detected the metadata can be sent to the DIA
using the Serial Number as the primary key value. A DET FQDN is
formed using the DET and used for the HIP RR and CERT RRs. Two CERT
RRs are required; one for the Self-Endorsement: UA sent in the
registration request, and one for the Broadcast Endorsement: DIME,
UA generated by the DPA. A Serial Number FQDN is used to create a
CNAME RR pointing to the DET FQDN.

A successful registration MUST return a HTTP code 200 with a payload
containing the following:

```
{
   "be": broadcast_endorsement,
   "serial_fqdn": "<id>.<mfr_code>.mfr.hhit.arpa."
   "hhit_fqdn": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa."
}
```

The broadcast_endorsement in the response is a Broadcast
Endorsement: DIME, UA.

3.2. Operator / Ground Control Station (GCS)

```
{
   "se": self_endorsement,
   "metadata": {
       ...
    }
}
```

The self_endorsement in the request is a Self-Endorsement: Operator
or Self-Endorsement: GCS.

A successful registration MUST return a HTTP code 200 with a payload
containing the following:

```
{
   "e": endorsement,
   "hhit_fqdn": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa."
}
```

The endorsement in the response is a Endorsement: DIME, Operator or
Endorsement: DIME, GCS.

3.3. Session ID

```
{
    "e": endorsement,
    "me": mutual_endorsement,
    "metadata": {
        "serial": "Serial Number",
        "uas_id": "base16 HHIT/DET of UA",
        "utm_id": UUIDv4,
        "utm_src": URI,
        "operator_det": "base16 HHIT/DET",
        "operator_id": "CAA Operator ID"
     }
}
```

The endorsement in the request is an Endorsement: Operator, UA or a Endorsement: GCS, UA. The mutual_endorsement in the request is Mutual Endorsement: DIME, Operator or a Mutual Endorsement: DIME, GCS. When the e and me are on or with an Operator then the operator_det MUST match the HHIT/DET found in those endorsements.

A successful registration MUST return a HTTP code 200 with a payload containing the following:

```
{
    "be": broadcast_endorsement,
    "e": endorsement,
    "hhit_fqdn": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa."
}
```

The broadcast_endorsement in the response is a Broadcast Endorsement: DIME, UA.

The endorsement in the response is an Endorsement: DIME, Operator, UA or an Endorsement: DIME, GCS, UA.

3.4. Child DIME

```
{
    "se": self_endorsement,
    "metadata": {
        "name": "",
        "abbreviation": "",
        "mfrCode": ""
        "addr": {
            "street1": "",
            "street2": "",
            "city": "",
            "sp": "",
            "pc": "",
            "cc": ""
        },
        "voice": "",
        "email": ""
    }
}
```

> Note: the mfrCode field is only used by an MRA when registering with an IRM and holds the ICAO assigned Manufacturer Code for [CTA2063A].

A successful registration MUST return a HTTP code 200 with a payload containing the following:

```
{
   "be": broadcast_endorsement,
   "e": endorsement,
   "hhit_fqdn": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa."
}
```

The broadcast_endorsement in the response is a Broadcast Endorsement: Parent DIME, Child DIME.

The endorsement in the response is an Endorsement: Parent DIME, Child DIME.

4. References

4.1. Normative References

[drip-detim] Wiethuechter, A., Card, S. W., Moskowitz, R., and J. Reid, "DRIP Entity Tag (DET) Identity Management Architecture", Work in Progress, Internet-Draft, draft-wiethuechter-drip-detim-arch-00, 27 September 2022, <https://www.ietf.org/archive/id/draft-wiethuechter-drip-detim-arch-00.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>.

[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>.

[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/info/rfc9153>.

4.2. Informative References

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

[drip-rid] Moskowitz, R., Card, S. W., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-Draft, draft-ietf-drip-uas-rid-01, 9 September 2020, <https://www.ietf.org/archive/id/draft-ietf-drip-uas-rid-01.txt>.

Appendix A. OpenAPI Specification

TODO

Authors' Addresses

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

Email: adam.wiethuechter@axenterprize.com

Stuart Card
AX Enterprize, LLC
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

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

Email: rgm@labs.htt-consult.com