Workgroup: drip Working Group
Internet-Draft:
draft-wiethuechter-drip-dia-http-00
Published: 27 September 2022
Intended Status: Standards Track
Expires: 31 March 2023
Authors: A. Wiethuechter
AX Enterprize, LLC
S. Card
AX Enterprize, LLC
R. Moskowitz
HTT Consulting

DRIP Information Agent (DIA) HTTP Interface

Abstract

This document defines an HTTP based interface using either JSON or CBOR for object encodings for the DRIP Provisioning Agent (DPA) or Registry to insert, update or delete information from a DRIP Information Agent (DIA). JSON Web Tokens (JWTs) are used between the entities to encapsulate and authenticate the transactions.

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.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The DIA 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 DIA MUST:

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

This document is the definition of this interface and its behavior; specifically between the DIA and a DPA or DIA and a Registry. 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. JWT Use

When using the JWT the iss is filled with the DET FQDN of the DIME component (typically the DPA). The sub is filled with the FQDN of the entity being registered. For a Serial Number this is the Serial Number FQDN of the UA, for the Operator/GCS the DET FQDN of the Operator/GCS and for the Session ID this is the DET FQDN of the UA.

A data field is filled with specific information to be stored in the RDDS by the DIA for the given subject.

Another field drip is used to hold various DRIP information elements.

The JWT is signed using the private key (an EdDSA25519 key) of the iss entity; the DPA.

4. 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.

4.1. Serial Number

```
{
    "iss": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "sub": "<id>.<mfr_code>.mfr.hhit.arpa",
    "iat": 0,
    "exp": 0,
    "drip": {
        "det": "base16 HHIT/DET",
        "hi": "base64 HI",
        "endorsements": [
            self_endorsement,
            broadcast_endorsement
        ]
    },
    "data": {
        "serial": "Serial Number",
        "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"
    }
}
```

Note: the drip field is optional.

4.2. Operator

```
{
    "iss": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "sub": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "iat": 0,
    "exp": 0,
    "drip": {
        "det": "base16 HHIT/DET",
        "hi": "base64 HI",
        "endorsements": [
            self_endorsement,
            endorsement
        ]
    },
    "data": {
        "name": "",
        "addr": {
            "street1": "",
            "street2": "",
            "city": "",
            "sp": "",
            "pc": "",
            "cc": ""
        },
        "voice": "",
        "email": "",
        "part107": "",
        "recFlyerId": ""
    }
}
```

4.3. Ground Control Station (GCS)

```
{
    "iss": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "sub": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "iat": 0,
    "exp": 0,
    "drip": {
        "det": "base16 HHIT/DET",
        "hi": "base64 HI",
        "endorsements": [
            self_endorsement,
            endorsement
        ]
    },
    "data": {
        ...
    }
}
```

4.4. Session ID

```
{
    "iss": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "sub": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "iat": 0,
    "exp": 0,
    "drip": {
        "det": "base16 HHIT/DET",
        "hi": "base64 HI",
        "endorsements": [
            self_endorsement,
            broadcast_endorsement,
            mutual_endorsement,
            endorsement
        ]
    },
    "data": {
        "serial": "Serial Number",
        "session_id": "base16 HHIT/DET of UA",
        "utm_id": UUIDv4,
        "utm_src": URI,
        "operator_det": "base16 HHIT/DET",
        "operator_id": "CAA Operator ID"
    }
}
```

4.5. Child DIME

```
{
    "iss": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "sub": "<hash>.<oga_id>.<hda>.<raa>.<prefix>.hhit.arpa",
    "iat": 0,
    "exp": 0,
    "drip": {
        "det": "base16 HHIT/DET",
        "hi": "base64 HI",
        "endorsements": [
            self_endorsement,
            endorsement,
            broadcast_endorsement
        ]
    },
    "data": {
        "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 ANSI CTA2063-A Serial Numbers.

5. 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>.

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