drip Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

A. Wiethuechter
AX Enterprize, LLC

20 October 2025

Protocol for Crowd Sourcing Air Domain Awareness
draft-wiethuechter-drip-csada-00

Abstract

This document standardizes an architecture to enable trust to sensors that provide Air Domain Awareness. Broadcast Remote ID is used as the primary example to define data models and methods used.

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 23 April 2026.

Table of Contents

1. Introduction

> Note: This document is directly related and builds from [MOSKOWITZ-CSRID] expanding it to be more general for ADA. That draft is a "top, down" approach to understand the concept and high level design. This document is a "bottom, up" implementation of the CS-RID concept. The content of this draft is subject to change and adapt as further development continues.

1.1. Purpose

Air Domain Awareness (ADA) is an important part of safe operations for aviation.

While this document will focus on adding Broadcast RID for ADA to UTM, the concepts, models and methods in this document can be expanded and used in other domain areas.

1.2. Background

TBD

1.3. Scope

This document uses Broadcast RID as a titular example to define a basic architecture and initial method of providing sensor data to UTM in a way that enables trust. This specific scenario is referred to as Crowd Sourced RID (CS-RID).

2. 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.

2.1. Additional Definitions

This document uses terms defined in [RFC9153] and [RFC9434] as well as those defined below.

Finder: Device acting as a sensor of one or more inputs in a domain. For this document the domain is aviation with the inputs being of various types such as audio, video, radio frequency, etc.

Supplemental Data Service Provider (SDSP): A server that Finders report updates to and acts as a gateway into UTM.

Web Token: An encapsulation mechanism for data. Can be either a CBOR Web Token (CWT, [RFC8392]) or JSON Web Token (JWT, [RFC7519]).

3. Architecture

With the initial use case of providing Broadcast RID for ADA to UTM this architecture closely follows and integrates into the wider UTM. See Appendix A of [RFC9434] for more information. All data models in this document are defined in the Concise Data Definition Language (CDDL, [RFC8610]).

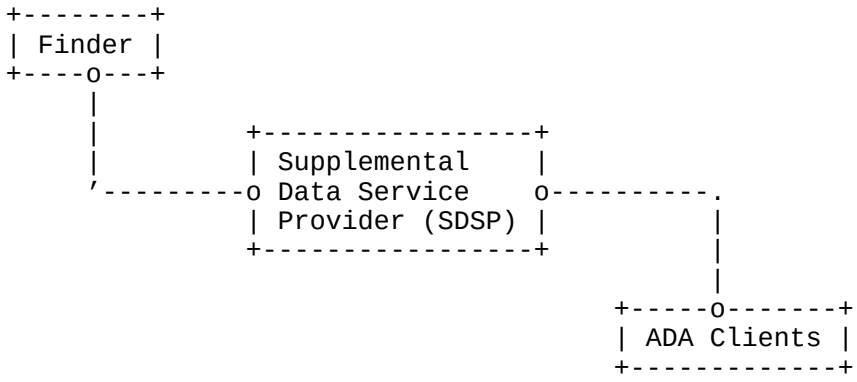

Figure 1: Simplified Architecture for Crowd Sourced ADA

Author TODO: expand Figure 1 to showcase different Finder sources and optional SDSP-to-SDSP interactions.

In this architecture the SDSP depends upon Finders to provide data via its "ingress" and exposes to clients on its "egress" data that has been filtered, aggregated and/or fused.

For CS-RID, defined in Section 4, Finders report a mix of raw detections or pre-processed UAS data (detected from Broadcast RID) to the SDSP to be further refined and translated to Network RID for UTM Clients.

Links between the SDSP and other entities is assumed to be bi-directional unless otherwise noted by a specific use-case. It is up to a given sensor use case to determine more in depth interaction models between the entities.

SDSPs can redirect "ingress" reports with unknown data elements if it knows another SDSP under the same ADA ecosystem that will process those unknown elements. An SDSPs "egress" may feed into another SDSP for further aggregation/fusion with other data sources.

It is RECOMMENDED that all participating entities of this ecosystem have a DRIP Entity Tag (DET, [RFC9374]) to enable between the parties during all interactions.

3.1. Reporting

```
report = {
  reporter_id: bstr / tstr / #6.54 / uuid,
  report_window: [
    start: tdate / time,
    end: tdate / time / uint
  ],
  ? brid: [+ detection],
  ? uas: [+ uas_datum],
  ? gnss: gnss_datum,
  ? reporter => reporter-datum,
  ? status => status-datum,
  * &(tstr, int) => any
}
```

Figure 2: Reporting Model

The reporting model Figure 2 is primarily used between the Finder and SDSP but MAY be used between SDSP and its clients. A report is filled with various different models under unique keys.

This document defines required report keys and models for CS-RID in Section 4 and additional OPTIONAL ones in Appendix B.

3.2. Encapsulation & Transporting

Reports MUST be authenticated and SHOULD be encrypted by its original source. These attributes can come from the combination of the transport and the application layer between the source and destination party. At the application layer the report can be encapsulated in a Web Token to provide both of these attributes.

Selection of certain transports can also securely enable for the SDSP to "push" information to Finders, such as provisioning and filtering requests. This problem can be considered a "configuration" problem, thus bringing a number of different alternatives to be used to solve rather than creating another domain specific solution. This problem, while noted, is out of scope for this document.

Selection of transport and supported interactions for given use-case, other than Broadcast RID, are out of scope for this document.

3.2.1. Web Token Encapsulation

The use of Web Token is RECOMMENDED when the transport layer does not provider either authentication of the source or encryption capabilities. Hosts SHOULD use a DET as the kid in the Web Token but MAY provider either a different kid or place the public key directly in the Web Token header.

3.2.2. HTTPS Transport

When using the HTTPS transport Reports MUST be encapsulated in a Web Token as described in Section 3.2.1 to provide client authentication and encryption. It is RECOMMENDED that the SDSP serve their endpoints under /.well-known/csada for interoperability. Support for both Web Token encodings is RECOMMENDED.

The use of Mutual TLS Section 7.4.6 of [RFC5246] as part of the HTTPS exchange has not been explored for this architecture, but is theoretically possible for small and large scale deployments in both public and private domains when using the DRIP Key Infrastructure X.509 (DKIX).

3.2.3. HIP Transport

The Host Identity Protocol (HIP, [RFC7401]) can be used and provides, via the Base Exchange (BEX), authentication and encryption for both parties. DETs MUST be used and Reports MUST be CBOR encoded.

3.2.4. CoAP Transport

The Constrained Application Protocol (CoAP, [RFC7252]) is another supported transport that can provide both parties authentication and encryption. DTLS [RFC9147] is RECOMMENDED for use and MUST use the DET, and the Report MUST be sent encoded in CBOR. When using UDP, Reports MUST be encapsulated in a CWT per Section 3.2.1. Use of ./well-known/cs-ada/ similar to HTTPS is encouraged.

4. Crowd Sourced Remote ID

This document defines two data models, Section 4.1 and Section 4.2, to be used between the Finder and SDSP. The UTM, RID data encapsulation and transportation is already standardized with an overview provided in Appendix A.

For CS-RID, Finders and SDSP MUST support Web Tokens over HTTPS (Section 3.2.2) as the primary encapsulation and transport method. The other defined transports in Section 3.2 MAY be supported by an SDSP. Interactions started by the SDSP to the Finder are out of scope for this document with that link (Finder to SDSP) expected to be unidirectional.

4.1. Detection Report

```
detection = [
  reporter_position: #6.103 / null,
  detection_time: tdate / time,
  antenna: [ + antenna-info],
  transport: &transport-enum,
  mac_address: #6.48,
  message_counter: uint,
  brid_message: bstr,
  compliance: [* uint]
]

antenna-info = [
  frequency: number / null,
  sector: tstr / null,
  rssi: number
]
transport-enum = (
  0: UKN, 1: BLE, 2: BLR, 3: BCN, 4: NAN, 5: SIK
)
```

Figure 3: Detections Model

4.2. UAS Datum Report

```
uas_datum = [
  reporter_position: #6.103,
  transports: {
    + &transport-enum: [+ mac_address: #6.48]
  },
  datum: {
    ? timestamp => utc,
    ? uas_type => 0..15,
    ? uas_ids => [
      + [
        id_type: 0..15,
        uas_id: uas-id
      ]
    ],
    ? ua_status => 0..15,
    ? ua_position => [
      lla: position,
      barometric_altitude: number / null
    ],
    ? ua_bearing => uint,
    ? ua_speed => [
      vertical: number / null,
      horizontal: number / null
    ],
```

```
      ? ua_height => [
        agl: bool,
        height: number
      ],
      ? accuracy => [
        vertical: 0..15,
        horizontal: 0..15,
        altitude: 0..15,
        barometric: 0..15,
        timestamp: 0..15
      ],
      ? auth => [
        + [
          auth_type: 0..15,
          data: auth-data
        ]
      ],
      ? self_id => [
        desc_type: 0..255,
        desc: tstr .size 23
      ],
      ? fixed_operator_position => position,
      ? gnss_operator_position => position,
      ? take_off_position => position,
      ? classification => [
        region: 0..8,
        category: 0..15,
        class: 0..15
      ],
      ? area => [
        count: 1..255,
        radius: number,
        floor: number,
        ceiling: number
      ],
      ? operator_id => [
        operator_type: 0..255,
        operator_id: tstr .size 20
      ],
      ? compliance => [+ uint]
    }
  ]

  transport-enum = (
    0: UKN, 1: BLE, 2: BLR, 3: BCN, 4: NAN, 5: SIK
  )
```

Figure 4: UAS Datum Model

5. DRIP Requirements Addressed

This document addresses the following requirements from [RFC9153]: GEN-5 (Gateway)

6. IANA Considerations

6.1. Well-Known URIs

IANA is requested to add the following entries in the "Well-Known URIs" registry [WELL-KNOWN].

URI Suffix	Change Controller	Reference	Status	Related Information
csada	IETF	This RFC	permanent	N/A

Table 1: Additions to Well-Known URIs Registry

7. Security Considerations

TBD

8. Privacy & Transparency Considerations

TBD

9. Acknowledgments

The Crowd Sourcing idea in this document came from the Apple "Find My Device" presentation at the International Association for Cryptographic Research’s Real World Crypto 2020 conference.

10. References

10.1. Normative References

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

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[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>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/rfc/rfc8392>.

[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>.

[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>.

10.2. Informative 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>.

[MOSKOWITZ-CSRID] Moskowitz, R., Card, S. W., Wiethuechter, A., Zhao, S., and H. Birkholz, "Crowd Sourced Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-crowd-sourced-rid-15, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-moskowitz-drip-crowd-sourced-rid-15>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/rfc/rfc7252>.

[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/rfc/rfc7401>.

[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>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[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>.

[WELL-KNOWN] IANA, "Well-Known URIs", July 2025, <https://www.iana.org/assignments/well-known-uris/>.

Appendix A. ASTM Network RID Overview

This appendix is normative and an overview of the Network RID portion of [F3411].

This appendix is intended a guide to the overall object of Network RID and generally how it functions in context with a SDSP supporting CS-RID. Please refer to the actual standard of [F3411] for specifics in implementing said protocol.

For CS-RID the goal is for the SDSP to act as both a Network RID Service Provider (SP) and Network RID Display Provider (DP). The endpoints and models MUST follow the specifications for these roles so UTM clients do not need to implement specific endpoints for CS-RID and can instead leverage existing endpoints.

An SDSP SHOULD use Network RID, as it is able, to query a USS for UAS sending telemetry in a given area to integrate into the Broadcast RID it is receiving from Finders. How the SDSP discovers which USS to query is out of scope for this document.

An SDSP MUST provide the Network RID DP interface for clients that wish to subscribe for updates on aircraft in the SDSP aggregated coverage area.

Appendix B. Additional Report Models

B.1. Global Navigation Satellite System (GNSS)

```
gnss_datum = [
  status: gnss-status,
  errors: [* gnss-error]
]
gnss-status = [
  timestamp: tdate / time,
  position: #6.103,
  dop: [
    hdop: number,
    vdop: number,
    pdop: number
  ] / null,
  fix: 0..3,
  bearing: number,
  speed: number,
  satellites_in_view: uint,
  satellites: [
    * [
      id: uint,
      snr: number,
      elevation: number,
      azimuth: number
    ]
  ]
]
gnss-error = [
  field: tstr,
  reported: any,
  threshold: any
]
```

Figure 5: GNSS Model

B.2. Reporter

```
reporter-datum = {
  serial: tstr,
  ? make: tstr,
  ? model: tstr,
  ? ip_addr: tstr / #6.52 / #6.54,
  * &(tstr, int) => any
}
```

Figure 6: Reporter Model

B.3. Finder Status

```
status-datum = {
  ? last_detect_time: tdate / time,
  * &(tstr, int) => any
}
```

Figure 7: Status Model

Author's Address

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