DRIP
Internet-Draft
Intended status: Standards Track
Expires: 20 October 2025

R. Moskowitz
HTT Consulting
S. Card
A. Wiethuechter
AX Enterprize
A. Gurtov
Link旦ping University

18 April 2025

Secure UAS Stateless Network RID
draft-moskowitz-drip-stateless-nrid-01

Abstract

This document defines a stateless transport mechanism and message content between an Uncrewed Aircraft System (UAS) and its UAS Service Supplier (USS) for Network Remote ID (Net-RID) messages. It leverages the Broadcast Remote ID (B-RID) messages as constructed by the UA, or constructed by the Ground Control Station (GCS) from the Command-and-Control (C2) messages that are then sent directly over UDP from the UAS. These messages are authenticated by the DRIP Authentication messages if originating from the UA. When originating from the GCS, CBOR Web Tokens (CWT) signed by the GCS's DRIP Entity Tag (DET), are used.

Transport privacy is out-of-scope in this approach per the stateless design. Some proposals are offered for data privacy that require some minimal state.

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 20 October 2025.

Table of Contents

1. Introduction

The ASTM Remote ID [F3411-22a] standard in Section 4.5 defines that there may be communications from the Uncrewed Aircraft System's (UAS) to its UAS Service Supplier (USS) Network Service Provider (Net-RID SP) to convey the Remote ID data. However, Section 4.5.4 specifically states the standard does not specify the details of this interface. This document provides the UAS to Net-RID SP interface for DRIP enabled UAS.

This document leverages the ASTM F3411 Remote ID broadcast messages to inform the Net-RID SP of the UA flight activity. This is realtime data transmission over a UDP connection between the UAS and USS.

Direct UDP with CoAP/CBOR ([RFC7252]/[RFC8949]) was selected for their low communication "cost". This may not be an issue if Net-RID originates from the Ground Control Station (GCS, Section 3.1.2), but it may be an important determinant when originating from the UA (Section 3.1.1). Particularly, very small messages may open Net-RID transmissions over a variety of constrained wireless technologies.

If a flight activity originates directly from the Uncrewed Aicraft (UA), the data is protected with DRIP Wrapper Messages Section 4.3 of [RFC9575]. This message may be directly transmitted from the UA to its Net-RID SP over some airborn Internet path, or it may be proxied through the UA's Ground Control Station (GCS). With the GCS in the loop, the GCS handles the Net-RID SP Heartbeat messaging. Other systems MAY act as a proxy for the UA, provided they are configured with a DET.

If a flight activity originates directly from the GCS, the GCS constructs the appropriate ASTM F3411 messages based on information it receives from the UA over the Command-and-Control (C2) link (e.g. derived from the MAVLink protocol [MAVLINK]). These messages are sent to the Net-RID SP in an ASTM F3411 Message Pack. The GCS's DET is used for the DRIP authentication in this case. The GCS handles all the USS Heartbeat messages.

The flight activity MAY originate from another Operator owned device (e.g. a smartphone). This is a device that is capable of receiving all the UA's transmissions and forward them to the Net-RID SP just as the GCS does. This will require this device to have its own DET known to the USS to be owned by the Operator.

1.1. Stateless Design Implications

Unlike the [FAA-UTM-ConOps-2.0] and [EU-UTM-ConOps-4.0] where they envision a stateful session between the NRID components. The approach here is stateless. The most compelling justification that is missed in the CONOPS is that there will often not be a single Net-RID SP server but a set of them. Thus major design consideration driving a stateless design is to support handoffs between multiple Net-RID SPs. Two major uses of multiple Net-RID SPs are:

Provide load balancing handoff between Net-RID SPs

Provide geographic diversity handoff as UA travels

Even in situations where a UA only communicates with a single Net-RID SP during an operation, the Net-RID SP may have a default, starting server for all operations and, based on a filed flight plan, immediately hand off the UA to the best server for that operation. The stateless design here gives the Net-RID SP extensive flexiblity in how this could be deployed.

There really is a very minimal piece of state, in that the UAS is transmitting to a specific Net-RID SP and said Net-RID SP is informing the UAS that it is receiving its messages. If the UAS does not get acknowledgments from its Net-RID SP, this MAY impact its CAA (Civil Aviation Authority) operation rules. Likewise if the Net-RID SP is not receiving the messages, it MAY need to flag the operation as ended.

This minimal state can be maintained through through a RESTFUL token included within the UDP messaging in place of a stateful TCP connection. To facilitate this, CBOR Web Tokens (CWTs) [RFC8392] are used.

Thus CWTs are used by the UAS to convey the flight activity and other information to the Net-RID SP. They are used by the Net-RID SP for its communication to the UAS.

1.2. SCHC Compression usage

To further reduce the communication cost, SCHC [RFC8724] is defined for both the direct UDP and CoAP layer [RFC8824].

UDP SCHC compression is handled separately here from IP header as is currently defined by IP carrier (e.g. LoRaWAN, [RFC9011]). This is to allow for the endpoints to not need to know what constrained carrier is in-path and just design for worst case.

1.3. Privacy Requires some State

Content privacy via a secure transport is out-of-scope for this protocol. Most secure transports are stateful, breaking the stateless approach taken here. It may seem that confidentiality is optional, as most of the information in Net-RID is sent in the clear in Broadcast Remote ID (B-RID), but this is a potentially flawed analysis. Net-RID has eavesdropping risks not in B-RID and may contain more sensitive information than B-RID. The secure transport for Net-RID should also manage IP address changes (IP mobility) for the UAS. Thus for some use cases a way to provide confidentiality is desirable.

CBOR Object Signing and Encryption (COSE) [RFC8152] may provide the simplest method to add data encryption to Net-RID. This may be developed at a later time.

Another approach that may be investigated later is the Object Security for Constrained RESTful Environments (OSCORE, [RFC8613]) protocol. OSCORE provides a CoAP compliant data encryption, but does not provide the session keys. The Messaging Layer Security (MLS, [RFC9420]) Protocol, may be well suited for the multiple Net-RID model used here and will be discussed further down.

2. Terms and Definitions

2.1. Requirements 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. Definitions

See Section 2.2 of [RFC9153] for common DRIP terms. The following new terms are used in the document:

B-RID
: Broadcast Remote ID. A method of sending RID messages as 1-way transmissions from the UA to any Observers within radio range.

Net-RID
: Network Remote ID. A method of sending RID messages via the Internet connection of the UAS directly to the UTM.

Net-RID SP
: Net-RID Service Provider. The specific component in the UTM system that provides the communication endpoint for a UAS. It may be a function within a USS, or at may be an external service to the USS.

RID
: Remote ID. A unique identifier found on all UA to be used in communication and in regulation of UA operation.

3. Network Remote ID

In UAS Traffic Management (UTM), the purpose of Net-RID is to provide situational awareness of a UA (in the form of flight tracking) in a user specified 4D volume. The data needed for this is already defined in [F3411-22a], but standard message formats, protocols, and secure communications methodologies are missing. F3411, and other UTM based standards going through ASTM and other SDOs, provide JSON objects and some of the messages for passing information between various UTM entities (e.g., Net-RID SP to Net-RID SP and Net-RID SP to Net-RID DP) but does not specify how the data gets into UTM to begin with. This document will provide such an open standard for DRIP enabled UAS.

A minimal messaging approach, using the Broadcast Remote ID (B-RID) messages in [F3411-22a], is sufficient to meet the needs of Net-RID. These messages can be sent to the Net-RID SP when their contents change. Further, a UAS supporting B-RID will have minimal development to add Net-RID support. The ASTM Message Pack (Msg Type 0xF) is used in all Net-RID messaging.

Other messages (e.g. Heartbeat) are needed in some Net-RID situations. Thus a simple message multiplexer using CWT over CoAP is defined for a richer messaging environment.

3.1. Network RID Endpoints

The US FAA defines the Network Remote ID endpoints as a USS Network Service Provider (Net-RID SP) and the UAS. Both of these are rather nebulous items and what they actually are will impact how communications flow between them.

The Net-RID SP may be provided by the same entity serving as the USS. This simplifies a number of aspects of the Net-RID communication flow. The Net-RID SP is likely to be stable in the network, that is its IP address will not change during an operation. This simplifies maintaining the Net-RID communications.

In practice, a USS may need multiple Net-RID SP, either for load balancing or geographical diversity. The design here is that the UAS communicates with one Net-RID SP server at a time. That SP server MAY redirect the UAS to use a different SP server via the HEARTBEAT message. It is this multiple Net-RID SP server design that mandates the stateless communication model and presents the confidentiality challenge.

The UAS component in Net-RID may be either the UA, GCS, or the Operator's Internet connected device (e.g. smartphone or tablet that is not the GCS). In all cases, mobility MUST be assumed. That is the IP address of this end of the Net-RID communication may change during an operation (generally called a flight or mission). The Net-RID mechanism MUST support this.

3.1.1. Net-RID from the UA

Some UA will be equipped with direct Internet access. These UA will also tend to have multiple radios for their Internet access (e.g., Cellular and WiFi). This protocol is agnostic as to which interface is used when for sending the Net-RID communications. Multi-interface transmissions MAY result in out-of-order packet delivery, thus the SP MUST be prepared to reorder the packets. All B-RID messages contain a timestamp, thus simplifying the reordering process.

Multicast (GEN-10 in [RFC9153]) over multiple Internet connection technologies MAY be used improve QOS (GEN-7 in [RFC9153]) for Net-RID.

The UA will send DRIP Wrapper messages of the current UA activity. These will be sent in a UA signed CWT that will add the SP DET.

3.1.2. Net-RID from the GCS

Many UA will lack direct Internet access, but their GCS are connected. The GCS is then acting as a gateway for the UA.

There are two sources of the RID messages for the GCS, both from the UA. These are UA B-RID messages, or content from C2 messages that the GCS converts to RID message format. The protocol stateless design is such that it is agnostic on how the GCS got the data.

In a constrained wireless environment for the UA that is not functioning autonomously (i.e., at least C2 traffic to the GCS), this approach may be the most economical. It only uses the wireless to send the UA status once, to the GCS, that then provides the Net-RID functionality.

3.1.3. Net-RID from the Operator

Many UAS will have no Internet connectivity, but the UA is sending B-RID messages and the Operator, when within RF range, can receive these B-RID messages on an Internet Connected device that can act as the proxy for these messages, turning them into Net-RID messages.

3.1.4. Net-RID from the Operator Smart Device

TBD

3.2. Network RID Protocol

Net-RID messaging is tied to a UA operation. During the operation, continuous location information is sent by the UA with any needed updates to static operation information.

There are four components of the Net-RID protocol:

1. Setup
2. Operation start time
3. UAS messaging
4. SP messaging

The later two are somewhat asynchronous. Note all participating elements are configured with DETs to participate and they will tend to be in the same Hierarchy ID (HID).

3.2.1. Network RID Protocol Setup

There are two steps in setting up a UAS to use the Net-RID protocol:

1. The operator configures the UAS with the Net-RID SP DET. This is done either the UA or GCS, but the one with Internet connectivity (hereafter the Gateway). (Note: Most likely this DET is in the same HID as the UA, so the operator can be prompted with the 1st 64 bits and need only enter the 64 hash bits.)
2. The Gateway queries DNS with the Net-RID SP DET.
    1. Gets the HDA Endorsement of the Net-RID SP DET and its IP address as of NOW.
    2. If no response or validation fails, something is wrong with entered DET.

3.2.2. Network RID Operation Start time

Net-RID connectivity start can be considered a pre-flight check, so appropriate actions during failures in this phase should be consistent with organization-specific, system-specific, and/or operation-specific pre-flight checklists.

All Operational data comes from the UA in a DRIP Wrapper packet. This is transmitted to the SP via the UAS component that has the Internet Connection (the Gateway). It is this element that packs the Wrapper into a CWT.

At Operation Start time:

1. The Gateway queries DNS with the Net-RID SP DET.
    1. It gets the HDA Endorsement of the Net-RID SP DET and its IP address as of NOW.
    2. If no response or validation fails, something is wrong with entered DET.
2. The UA sends its first packet to the Net-RID SP via the Gateway before operation commences.
    1. This is a "normal" DRIP Wrapper (Section 4.3 of [RFC9575]) and SHOULD contain messages with static content.
    2. Vector/Location SHOULD be included in this 1st packet, if room.
    3. This Wrapper is packed by the Gateway into a CWT with the SP DET for sanity check that the right SP is the recipient.
3. The Net-RID SP ACKs with an Net-RID Heartbeat (defined below).
    1. The first packet/Heartbeat exchange continues for 4 tries. No success, then no operation.
    2. Note that the Heartbeat MAY have a Net-RID SP redirect for load balancing, sending the UA off to a different SP server. The redirect includes the new Net-RID SP’s DET, IP addr, and Endorsement.

3. The Heartbeat flags will inform the UA as to what information the SP is lacking and the UA will send a Message Pack Wrapper with the requested information. If this includes a request for Self-ID and the UA has no Self-ID a Self-ID with null content is sent. The SP MUST ACK with a Heartbeat with updated flags.

4. The Operation Start Phase completes when UA receives Heartbeat with flags indicating no missing information.

3.2.2.1. Static Messages

For simplicity, a class of UAS information is called here "Static", though in practice any of it can change during the operation, but will change infrequently. This information is the contents of the B-RID Self-ID (Msg Type 0x3), Operator ID (Msg Type 0x5), and System Messages (Msg Type 0x4). This information can simply be sent in the same format as the B-RID messages. Alternatively the individual data elements may be send as separate CBOR objects.

The Basic ID (Msg Type 0x0) Message may be included as a static message if this information was not used for the secure setup. There may be more than one Basic ID Message needed if as in the case where the Japan Civil Aviation Bureau (JCAB) has mandated that the Civil Aviation Authority (CAA) assigned ID (UA ID type 2) and Serial Number (UA ID type 1) be broadcasted.

The information in the System Message is most likely to change during an operation. Notably the Operator Location data elements are subject to change if the GCS is physically moving (e.g. hand-held and the operator is walking or driving in a car). The whole System Message may be sent, or only the changing data elements as CBOR objects.

3.2.3. Network RID UAS Messaging

1. The UA sends its operational information in a DRIP Wrapper

    1. This Wrapper MUST contain a current Vector/Location Message.

    2. It SHOULD contain any other RID messages with changed content (e.g. System Message).

2. The Gateway wraps packs this into a CWT and forwards it to the Net-RID SP.

3. On receipt of a Net-RID SP Heartbeat

1. If no message was sent to the SP in the past N seconds, resends the last sent message.

2. If Heartbeat contains a Net-RID SP redirect information, resends the last sent message to the new SP.

4. If no Net-RID SP Heartbeat was received in the past M seconds.

1. Resends the last sent message.

2. If no Heartbeat after resending this last message 4 times, assume lost connection to SP and take appropriate action.

5. On end of Operation, sends an "End-of-Operation" CWT to the Net-RID SP

1. MUST receive a Heartbeat with corresponding "End-of-Operation" CWT; resends EoO otherwise.

3.2.3.1. Vector/Location Message

Many CAAs mandate that the UA Vector/Location information be updated at least once per second. Without careful message design, this messaging volume would overwhelm many wireless technologies. Thus to enable the widest deployment choices, a highly compressed format is recommended.

The B-RID Vector/Location Message (Msg Type 0x1) is the simplest small object (24 bytes) for sending this information in a Message Pack (Msg Type 0xF).

3.2.4. Network RID SP Messaging

The Net-RID SP SHOULD send regular "heartbeats" to the UAS. If the UAS does not receive these heartbeats for some policy set time, the UA MUST take the policy set response to loss of Net-RID SP connectivity. For example, this could be a mandated immediate landing. There may be other messages from the Net-RID SP to the UAS (e.g., call the USS operator at this number NOW!). The UAS MUST follow acknowledge policy for these messages.

If the Net-RID SP stops receiving messages from the UAS (Section 3.2.3), it should notify the UTM of a non-communicating UA while still in operation.

The Net-RID SP process flow is as follows:

1. The Net-RID SP sends a Heartbeat to a Gateway every P seconds.

1. Even if it received a message (other than EoO) within this time period.

2. The Heartbeat MAY contain Net-RID SP Redirect content.

2. If the SP sends R Heartbeats without receipt of a message from the UAS, assume loss connectivity and take appropriate action.

3. On receipt of an "End-of-Operation" CWT.

1. Sends Heatbeat with EoO content and closes operation.

3.2.5. CoAP Net-RID messages

The CoAP based Net-RID protocol is intended for a rich, bi-directional conversation between the UAS and USS. The USS, through the Net-RID SP, may compare actual UA progress against the filed flight plan and against other UA actual traffic. The USS may then send to the UAS recommended changes to the flight plan to de-conflict traffic or advise the UAS to avoid hazards (1st responder event, avoid space). The UAS may then negotiate changes to the plan, and act on them, as appropriate.

Note that this additional USS-to-UAS messaging functionality is not part of the current design and is out of scope for this document. This sort of advanced UAS behavior is envisioned as part of total UTM activities. Discussions now ongoing in UTM will provide the data models and transactional UAS/USS interactions, that will drive UAS communications past the Net-RID defined here toward a more functional CoAP Net-RID protocol.

There are three CoAP Net-RID currently defined:

Author’s Note: This section needs further work. At least (and probably more) uas-update needs the Net-RID SP DET and both need their DET signing.

```
uas-cwt = 6.18([
    protected: {
        alg: -8
    },
    unprotected: {
        kid: #6.54(bstr) // DET
    },
    claims: {
        sub: "NRID-UAS",
        nbf: 0,
        exp: 10,
        iat: 0,
        TBD1: [
          det_sp: #6.54,
          ? encoded: [
              uint .bits message_types, ? uint .bits auth_pages]
          data: bstr  ; F3411 Message Pack (Message Type 0xF)
        ]
    }
    signature: bstr .size(64)
])
message_types = &(
    basic: 0,
    location: 1,
    auth: 2,
    self: 3,
    system: 4,
    operator: 5,
    pack: 15
)
auth_pages = &(
    pg0: 0, pg1: 1, pg2: 2, pg3: 3,pg4: 4, pg5: 5, pg6: 6, pg7: 7,
    pg8: 8, pg9: 9, pgA: 10, pgB: 11, pgC: 12, pgD: 13, pgE: 14,
    pgF: 15
)
```

Figure 1: UAS CWT

```
uss-cwt = 6.18([
    protected: {
        alg: -8
    },
    unprotected: {
        kid: #6.54(bstr) // DET
    },
    claims: {
        sub: "NRID-USS",
        nbf: 0,
        exp: 10,
        iat: 0,
        TBD2: [
          det_uas: #6.54,
          expected: [
                       uint .bits message_types,
                       ? uint .bits auth_pages
                  ],
          ? move_sp: [
              new_sp: #6.54,
              new_ip: #6.54 / #6.52 / #6.32,
              new_be: bstr .size(136)
            ]
        ]
    }
    signature: bstr .size(64)
])
message_types = &(
    basic: 0,
    location: 1,
    auth: 2,
    self: 3,
    system: 4,
    operator: 5,
    pack: 15
)
auth_pages = &(
    pg0: 0, pg1: 1, pg2: 2, pg3: 3,pg4: 4, pg5: 5, pg6: 6, pg7: 7,
    pg8: 8, pg9: 9, pgA: 10, pgB: 11, pgC: 12, pgD: 13, pgE: 14,
    pgF: 15
)
```

Figure 2: USS CWT

```
eoo-cwt = 6.18([
    protected: {
        alg: -8
    },
    unprotected: {
        kid: #6.54(bstr) // DET
    },
    claims: {
        sub: "NRID-EOO",
        nbf: 0,
        exp: 10,
        iat: 0,
        TBD3: [ TBD ]
    }
    signature: bstr .size(64)
])
```

Figure 3: UAS End-Of-Operation

4. IANA Considerations

TBD

5. Security Considerations

TBD

TBD

6. Acknowledgments

TBD

7. References

7.1. 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/info/rfc2119>.

[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/info/rfc7252>.

[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>.

[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/info/rfc8949>.

7.2. Informative References

[EU-UTM-ConOps-4.0] Single European Sky ATM Research (SESAR), "EU U-Space CONOPS 4th Edition", February 2023, <https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20CONOPS%204th%20edition.pdf>.

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

[FAA-UTM-ConOps-2.0] US Federal Aviation Administration (FAA), "FAA Concept of Operations for Unmanned Aircraft Systems (UAS) Traffic Management (UTM) 2.0", March 2020, <https://www.faa.gov/sites/faa.gov/files/2022-08/UTM_ConOps_v2.pdf>.

[MAVLINK] "Micro Air Vehicle Communication Protocol", 2021, <http://mavlink.io/>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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/info/rfc8392>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[RFC8824] Minaburo, A., Toutain, L., and R. Andreasen, "Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)", RFC 8824, DOI 10.17487/RFC8824, June 2021, <https://www.rfc-editor.org/info/rfc8824>.

[RFC9011] Gimenez, O., Ed. and I. Petrov, Ed., "Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN", RFC 9011, DOI 10.17487/RFC9011, April 2021, <https://www.rfc-editor.org/info/rfc9011>.

[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>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/info/rfc9420>.

[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/info/rfc9575>.

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

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

Andrei Gurtov
Linkping University
IDA
SE-58183 Linkping
Sweden
Email: gurtov@acm.org