TMRID
Internet-Draft
Intended status: Standards Track
Expires: April 20, 2020

A. Wiethuechter
S. Card
AX Enterprize
R. Moskowitz
HTT Consulting
October 18, 2019

TM-RID Authentication Formats
draft-wiethuechter-tmrid-auth-00

Abstract

This document describes how to include HIPv2 into the proposed ASTM Remote ID specification defined in WK65041 by the F38 Committee under a Broadcast Remote ID (RID) scenario. It defines a few different message schemes that can be used to assure past messages sent by a UA and also act as a assurance for UA trustworthiness in the absence of Internet connectivity at the receiving node.

Table of Contents

1. Introduction

The technology space of Unmanned Aircraft (UA) has been expanding rapidly on numerous fronts. This rapid expansion has been noticed by various agencies and they are moving to add standards to protect individuals and organizations.

The ASTM has been selected to create a specification for Remote ID (RID) classification that various CAAs can cite. The work presented here is an expansion upon their standards to integrate IETF methods and work into the space where it is useful.

The current draft standard for Remote ID (RID) does not, in any meaningful capacity, address the concerns of trust in the UA space with communication in the Broadcast RID environment. This is a requirement that will need to be addressed eventually for various different parties that have a stake in the UA industry.

This document will show how UAS RID can be made trustworthy and can enable immediate encrypted communications between mutually authenticated parties (typically observer and pilot) by using the Host Identity Protocol Version 2 (HIPv2) [RFC7401].

Further, by leveraging the Hierarchical HIT (HHIT) [I-D.moskowitz-hip-hierarchical-hit] RID applications can be enabled to have trustworthiness for UA communication in the constrained environment of Broadcast RID.

This solution is called "Trustworthy Multi-purpose Remote ID".

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

CAA Civil Aeronautics Administration. An example is the Federal Aviation Administration; (FAA) in the United States of America.

C2 Command and Control.

RID Remote ID. Maximum length of 20 bytes.

HI Host Identity.

HIT Host Identity Tag.

HHIT Hierarchical Host Identity Tag.

UA Unmanned Aircraft.

UAS (Unmanned Aircraft System) Composed of Unmanned Aircraft and all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery

equipment, all required crew members, and command and control (C2) links between UA and the control station.

USS (UAS Service Supplier) USSs provide UTM services to support the UAS community, to connect Operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants. (From FAA UTM ConOps V1, May 2018).

3. UAS Problem Space

UA Systems (UAS) are usually in a volatile environment when it comes to communication. UA are generally small with little computational (or flying) horsepower to carry standard communication equipment. This limits the mediums of communication to few viable options. The ASTM standard focuses on two ways of communicating to a UAS for RID: Broadcast and Network.

3.1. Broadcast RID

Broadcast RID has three mediums of communication defined by the ASTM. These are: Bluetooth 4.X, Bluetooth 5.X Long Range, and Wifi with Neighbor Aware Networking (NAN).

A UA under the ASTM standard is required to support at least one of these methods to broadcast messages using the medium's respective advertisement framing methods. Note that when using Bluetooth 5 it must be transmitted concurrently with Bluetooth 4.X (which the ASTM refers to as Bluetooth Legacy).

The selection of the Broadcast medium was driven by research into what is commonly available on 'ground' units (smartphones and tablets) and what was found as prevalent or 'affordable' in UA. Further, there must be an API for the UAS receiving application to have access to these messages. It is worth noting that at this time, Bluetooth 4.X is readily available but the other two are more for future devices. Thus the focus on working within the 26 byte limit of the Bluetooth 4.X "Broadcast Frame" that goes out on the beacon channels.

Finally, the 26 byte limit of the Bluetooth 4.1 "Broadcast Frame" strictly enforces the RID maximum length of 20 bytes.

3.2. Network RID

Network RID is a much more open space and is enabled when a UA has Internet connectivity on board. This means, in most cases, the

inclusion of a cellular modem on board, but can include WiFi communications. Network RID is the subject of a future document.

3.3. TM-RID Focus Problem Space

This document will focus on adding trust to Broadcast RID. The ASTM proposed standard 'used' the limitation put onto the UA by its physical design and radio communications to leave one important issue un-addressed: Trust.

Further, the one-way, Adhoc, nature of Broadcast RID precludes any stateful security protocol to provide trust which further hampered any evaluation of Trust methodologies.

As currently defined by ASTM, any UA can announce a RID and an observer would be seriously challenged to validate the validity in the RID and thus any information about the UA. This is why trust in the RID and related trust for all Broadcast messages is considered critical in the safe operation of UAs.

4. Trustworthy Multi-purpose Remote ID

This document addresses this oversight by using HIP to bring trust into UA communication without having to redesign the standard. The Host Identity Tag (HIT) and Host Identity (HI) of HIP are used to provide signed statements of Trust of the broadcast messages. HIP, for Broadcast RID, is only used as in HHIT Registries [I-D.moskowitz-hip-hhit-registries] to prevent duplicate HHITs and provide the Registries with UA information for DNS and other inquires.

The use of HIP is strongly encouraged by the authors to be used in Network RID.

4.1. HIP Benefits for Remote ID

The Host Identity Tag (HIT) of HIP is unique among structured number Identifiers. It significantly more valuable as an Identifier than any other structured number in IETF standards, including [RFC6920] option of hash of Public Keys.

It is a valid IPv6 (non-routable) address. As such it can be used directly as addresses in applications.

The Suite ID field informs the receiver of the underlying cryptographic Identity.

The hash of the Host Identity public key provides the real proof of ownership of the HIT through any private key operation.

By using HIP a number of benefits to UAs are immediately enabled:

Unique Identification: Using the HIP's Host Identity Tag (HIT) a unique identifier can be used as a handle for more information than just PII.

Immediate UA Context: The Hierarchical Host Identity Tag (HHIT) provides provable context about the Identity.

Automatic Connectivity: When both devices are using HIP the HIT can be used, along with standard DNS methods, to quickly create secure connections between hosts. This applies even when both end-points are mobile in nature.

4.2. Levels of Trust

TM-RID for Broadcast RID there are three levels of trust:

Level 1 (Identification): The HHIT is a unique identifier that can enable other levels of TM-RID while still fitting within the specification of the standard for ID fields.

Level 2 (Authentication): When a HHIT is used for an ID of a UA a lookup to other information is easy and already has infrastructure to do so in place.

Level 3 (Communication): After looking up information using a HHIT dynamic communication to other parties can be performed that is secure and trusted. (Note that this is for Network RID.)

4.2.1. TM-RID Level 1 (Identification)

Level 1 uses HHIT as an ID type in the ASTM standard. This gives no immediate effects of HIP or trust for the UA, but can enable further features in other levels.

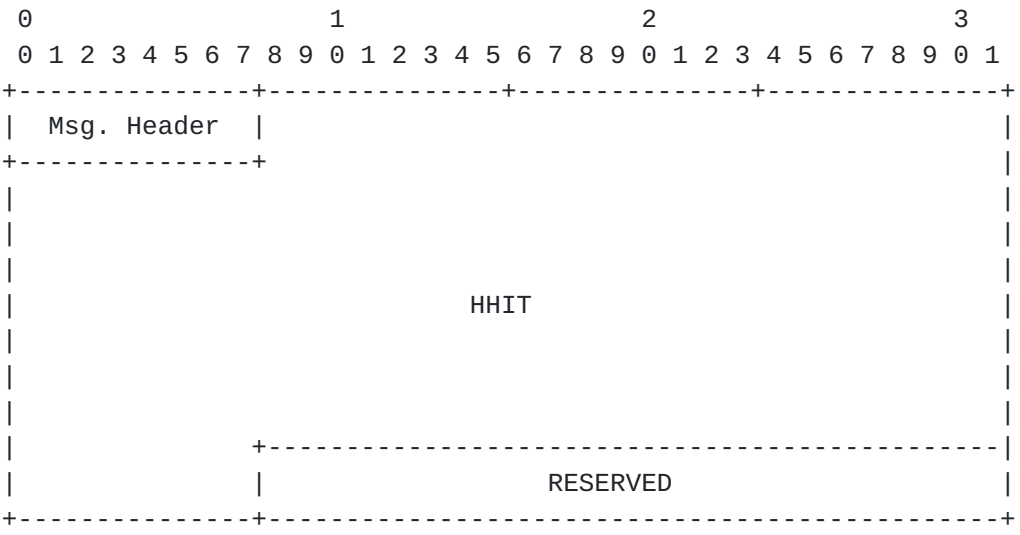
Under the current proposed standard (which does not include HIP as a valid entry for ID type) the ID type of "4" should be used in the Basic ID Message to signal the use of a HHIT as the ID.

At the time of writing Type 4 in the ASTM standard has yet to used, there is no definition for Private used ID types in the standard to use.

The RID ONLY is sent in the Basic ID Message. The standard relies on the MAC address to relate all messages from a UA to this RID.

Level 1 does not provide any trust in the RID. The Basic ID Message is limited to 24 bytes and can only carry the, at maximum 20 byte, RID.

Below is an example of a ASTM Basic ID message format using HHIT as the UAS ID type.



Msg. Header (1 byte)
Contains two subfields: ID Type and UA Type (of 4 bits each). In the above example the ID Type would be set to "0100".

4.2.2. TM-RID Level 2 (Authentication)

With Level 2 it is assumed that the receiving application being used by the observer has encountered a HHIT in a Basic ID Message.

A HHIT can be used to construct a FQDN that can be used in a DNS query that will minimally provide the HI for validating signed Broadcast Authentication Messages.

This construction may be through a reverse lookup using the HHIT as an IPv6 address. It may be through an FQDN construction method imposed on the receiving application by the receiving application's USS.

A Suite ID of EdDSA [I-D.moskowitz-hip-new-crypto] with the EdDSA25519 curve is used as its 64 byte signature will fit in the Authentication Messages.

Besides the HI, the most common case will most likely yield a pointer of some kind to be used in a controlled access controlled database to obtain PII.

4.2.3. TM-RID Level 3 (Communication)

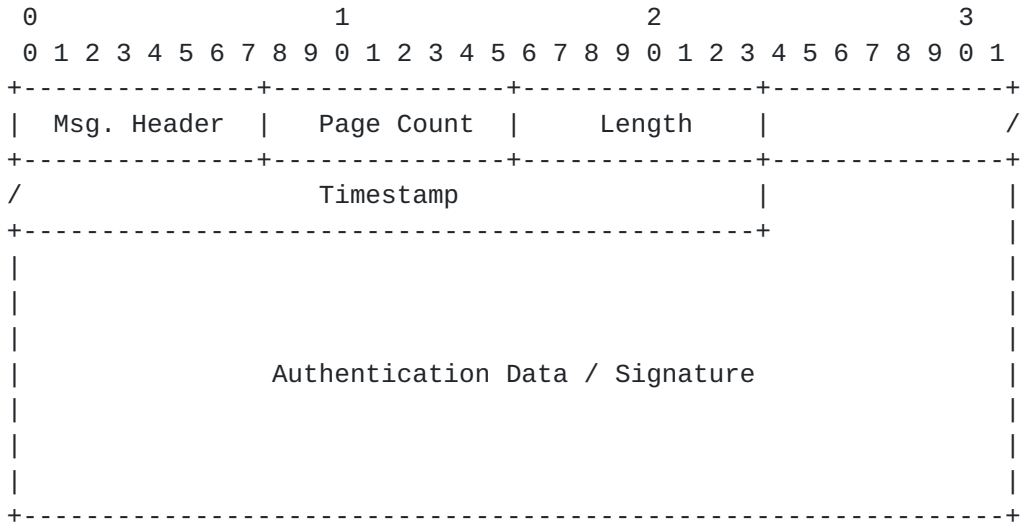
Under Level 3 the HHITs, along with Rendezvous Servers (RVS) and other HIP aware/enabled infrastructure, would be used as intended to connect two hosts securely.

This will be the subject of the Network RID document(s).

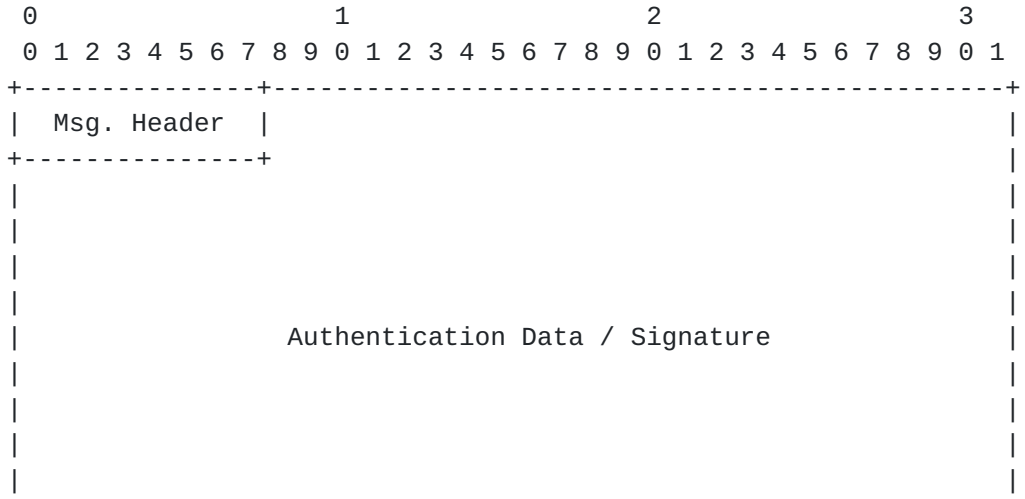
5. ASTM Authentication Message

The ASTM Authentication Message format is defined as follows:

Page 0:



Page 1 - 4:



```
+------------------------------------------------------------+
```

Msg. Header
: A byte field containing two 4 bit fields. Authentication Type and Page Number.

Page Count
: Only on page 0. Total number of pages this authentication message has. Max value of 5.

Length
: Total length of Authentication Data / Signature in bytes. Value of 0 - 109.

Timestamp
: 32 bit Unix timestamp since 00:00:00 01/01/2019.

Authentication Data / Signature
: Opaque authentication data.

A few important things to note on this format and its constraints.

1. Each page has only 24 bytes based on the Bluetooth 4.X/5.X specification.

2. The limit on Page Count of 5 is based on being able to fit this message as well as 5 other messages (each capped at 25 bytes) into a Bluetooth 5 atomic message. The intention is that this message authenticates the whole pack.

6. HIP Based Extensions to the ASTM Authentication Message

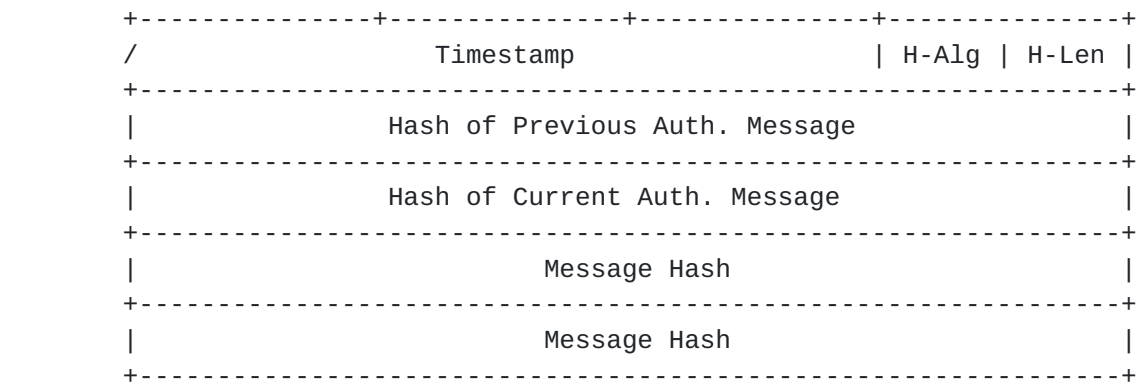
The following section describes various methods that HIP can help enable more trustworthy communication using the Authentication Message as the base. Each diagram will show all 5 pages of the format filled out as examples.

6.1. Signed Hash Lists

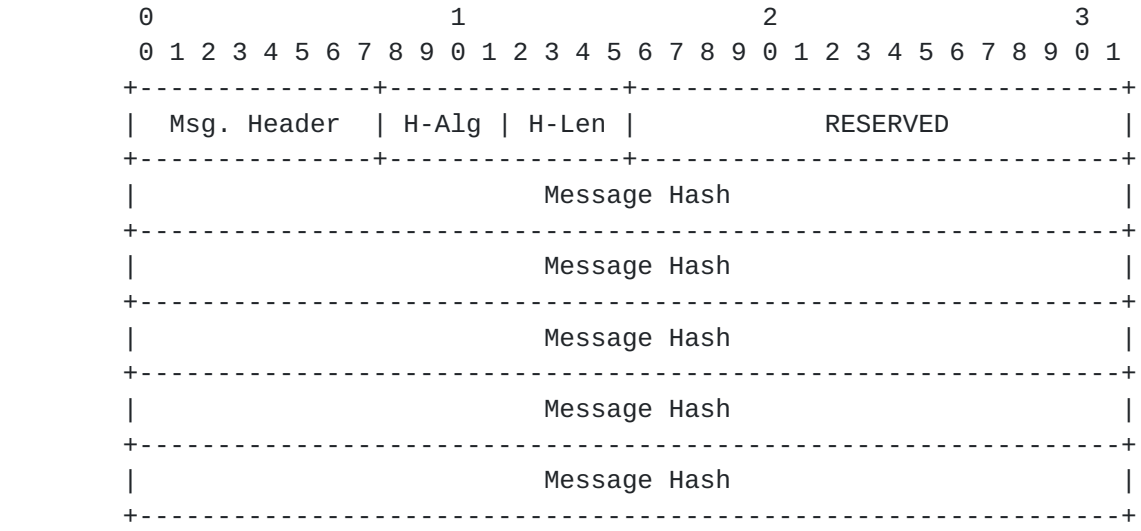
This format is designed to provide provenance to Broadcast RID messages sent by a give UAS.

Page 0:

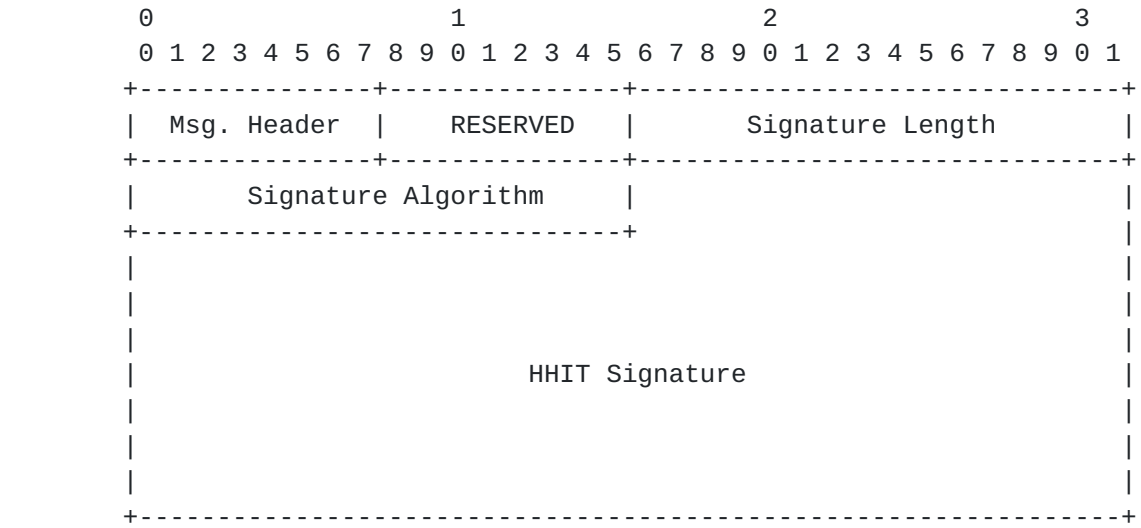
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|  Msg. Header  |   Page Count  |     Length    |               /
```



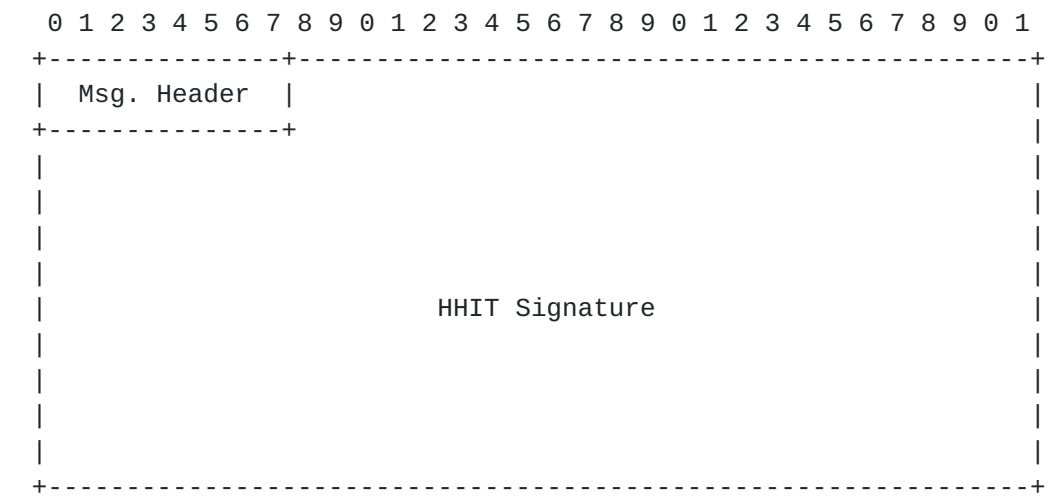
DataPage 1:



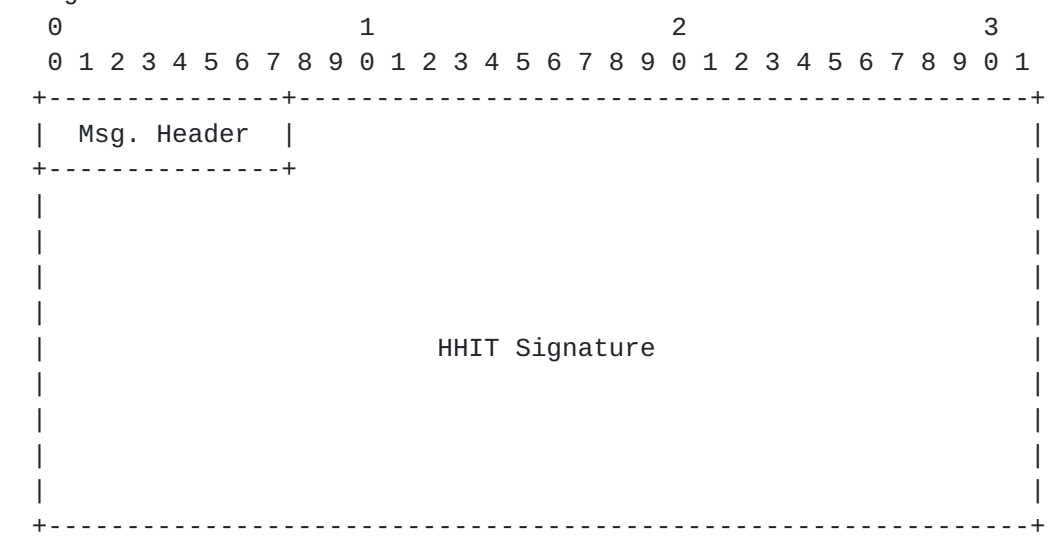
Page 2:



Page 3:



Page 4:



H-Alg, H-Len: (4 bits), (4 bits)
These are fields for relaying information of the Hash algorithm used for the messages and the Hash length (in octets). For this example of the format a length of 4 bytes is used.

Hash of Previous Auth. Message: (4 bytes)
A hash of the previous send Authentication message.

Hash of Current Auth. Message: (4 bytes)
A hash of the current Authentication message.

Message Hash: (4 bytes)
A hash of a previously sent message.

Signature Length: (2 bytes)

Length of signature in octets, excluding Length, and Padding

Signature Algorithm: (2 bytes)
Self explanatory.

HHIT Signature: (64 bytes)
EdDSA25519 signature using an EdDSA25519-based HHIT from HIP. Spread across 3 pages of a given DataPage.

This specific format has various different ways to be added into the Authentication Message structure - the general concept is the same regardless.

By hashing previously sent messages and signing them we gain trust in the UAS's previous reports. An observer who has been listening for any length of time can hash received messages and cross check against listed hashes. The signature is signed across the list of hashes.

Two special hashes are included; a previous authentication hash, which links to the previous signed hash list message, as well as a current hash. This gives a pseudo-blockchain provenance to the authentication message that could be traced back if the observer was present for extended periods of time.

In regards to the creation and use of the current authentication hash field:

First during creation and signing of this message format this field MUST be set to 0. So the signature will be based on this field being 0, as well as its own hash. It is an open question of if we compute the hash, then sign or sign then compute.

There a few different ways to cycle this message. We can "roll up" the hash of 'current' to 'previous' when needed or to completely recompute the hash. This mostly depends on the previous note.

6.1.1. Limitations

With the current format defined by ASTM only 7 messages can be hashed reasonably in the above format.

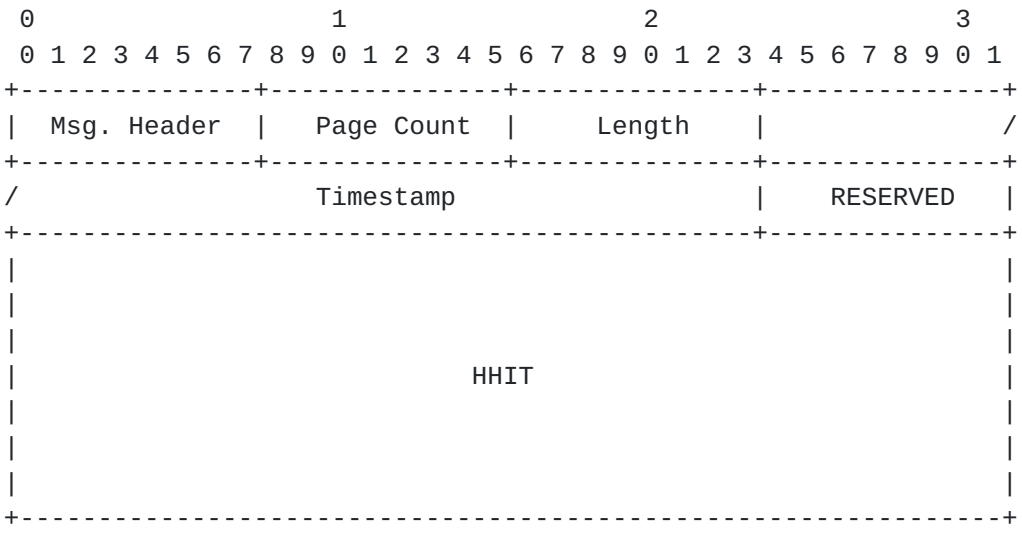
Another option is to places hashes into the Authentication Wrapper format (also defined in this document). This only gives five total hashes - excluding the pseudo-blockchain linking hashes entirely.

To address this problem the authors feel that the Authentication Messages needs to have a max bound of 10 pages, instead of 5. This argument is discussed later in this document.

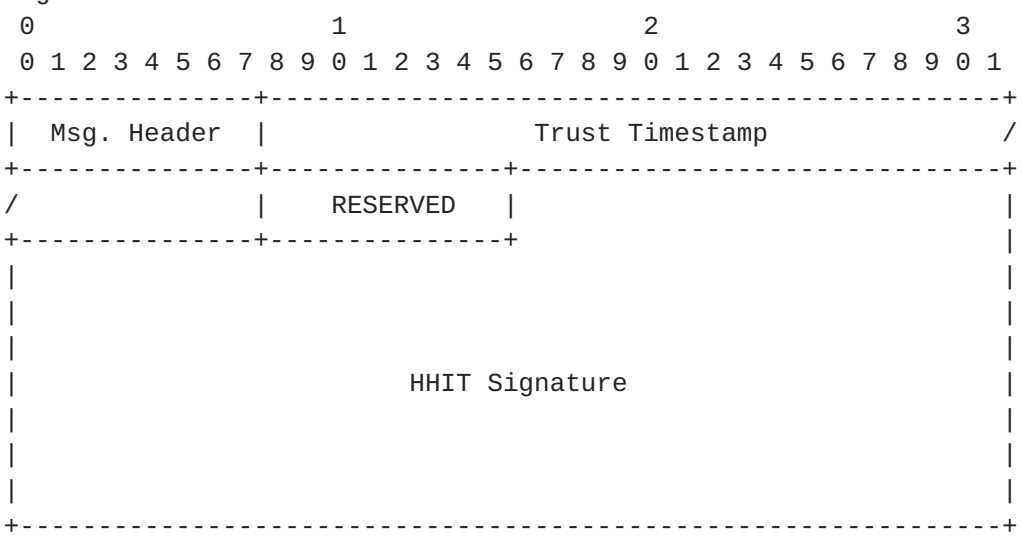
6.2. HIP Based Authentication Wrapper

This format is a way to authenticate a given UA using the first 2 levels of TM-RID for UAS.

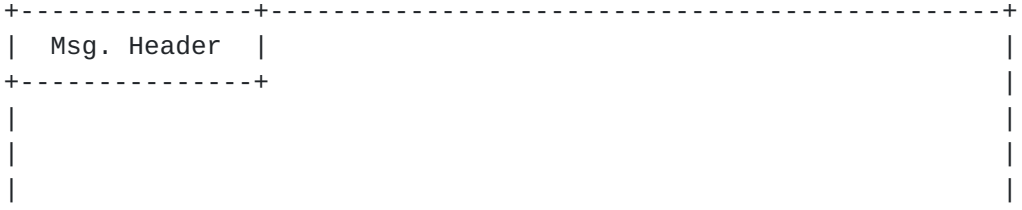
Page 0:

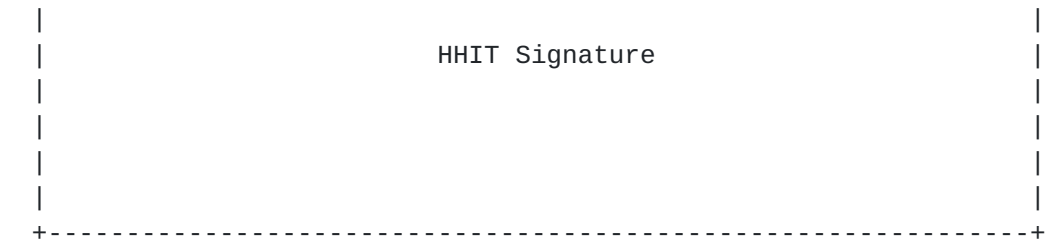


Page 1:

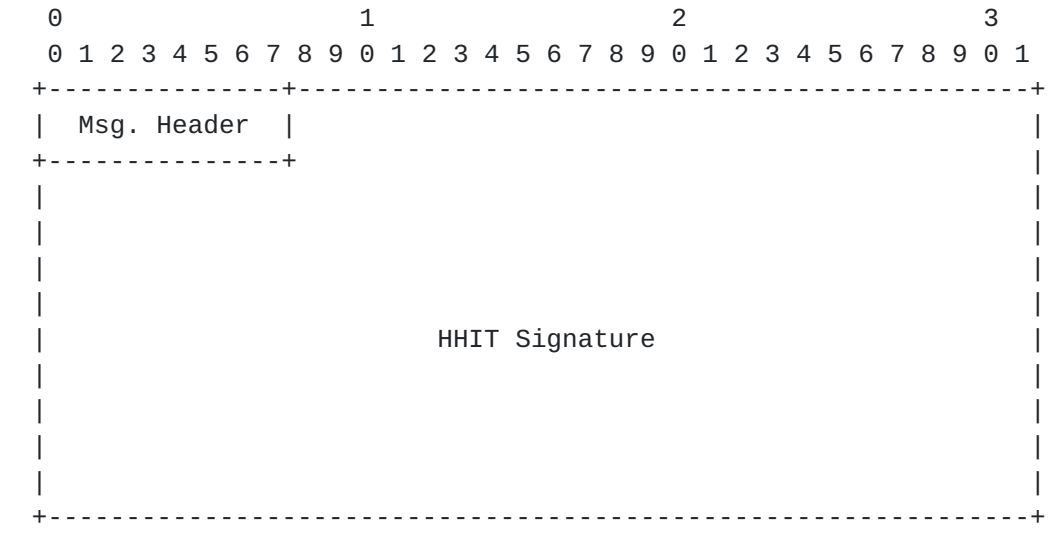


Page 2:

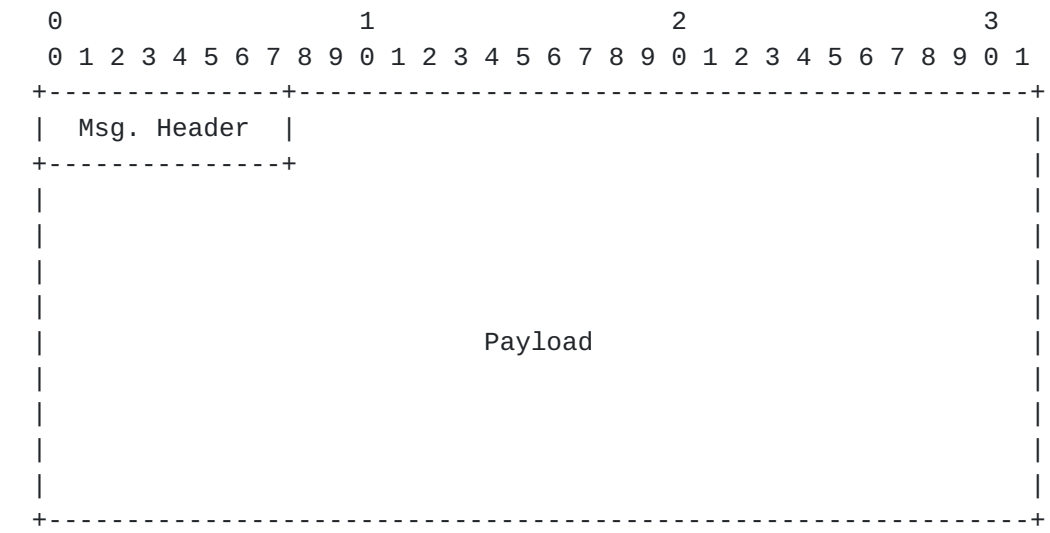




Page 3:



Page 4:



HHIT

16 byte HHIT of EdDSA25519 HI.

Trust Timestamp

4 byte message trust until timestamp.

HHIT signature
: 64 byte Signature of whole message.

Payload
: 0 to n bytes of payload. Max of n is 23.

In this format the Payload could be anything that fits within the 23 bytes. A further two btyes could be used for payload (by removing) the RESERVED sections allowing for 25 bytes of payload.

6.2.1. Specific Use Case: Trusted Messages

This document suggests the creation of a "Trusted Message".

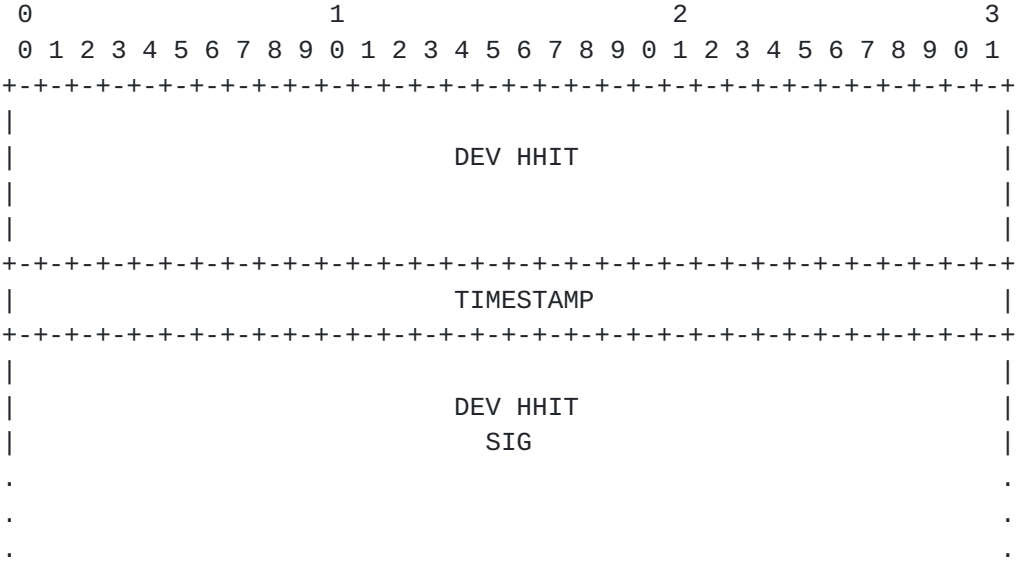
One specific use case that is useful in the RID space is the creation of a "Trusted Vector Message". By placing a previous [or new] vector message into the Payload section of the Authentication Message a verifiable broadcast can be created.

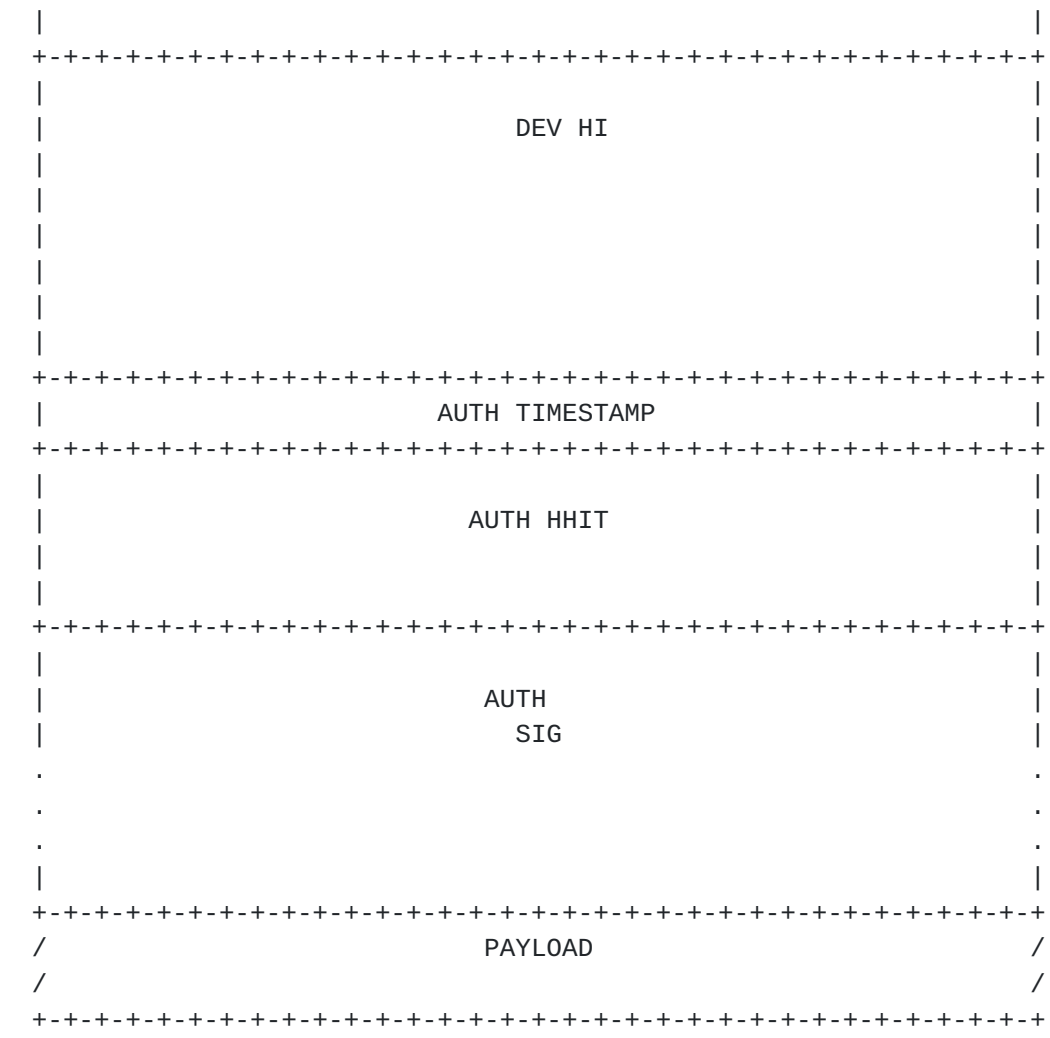
Due to being signed this creates an authentic vector that is hard to spoof, which can confirm flight paths in real time.

This model can be applied to any of the Broadcast RID messages in the ASTM standard as they all fit within the max of 25 bytes.

6.3. HIP Based Offline Authentication

This specific format does not currently fit within the ASTM specification. Requiring a minimum of 200 bytes, this would require the Authentication Message to have 10 pages, instead of the current 5 page limit.





DEV HHIT	16 byte Dev HHIT of EdDSA25519 HI
TIMESTAMP	4 byte packet trust until timestamp
DEV HHIT SIG	64 byte Signature of whole packet
DEV HI	32 byte Device HI of EdDSA25519 HI
AUTH TIMESTAMP	4 byte Dev HHIT trust until timestamp
AUTH HHIT	16 byte Authorizer's HHIT of EdDSA25519 HI
AUTH SIG	64 byte Signature of Device HHIT-HI
PAYLOAD	0 to n bytes of payload
Length	200 + n bytes

What this will grant, if attainable in future revisions of the ASTM specification, is the ability to authenticate UA information when the receiving device of the observer (e.g. a smartphone with a dedicated RID application) has no Internet service (e.g. LTE signal).

By including the device HI along with a signature from the registry the UA is under, we can assert trust of a given drone without requiring the need for immediate reverse lookups online.

7. IANA Considerations

TBD

8. Security Considerations

TBD

9. Acknowledgments

TBD

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/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>.

10.2. Informative References

[I-D.moskowitz-hip-hhit-registries] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HIT Registries", draft-moskowitz-hip-hhit-registries-01 (work in progress), October 2019.

[I-D.moskowitz-hip-hierarchical-hit] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", draft-moskowitz-hip-hierarchical-hit-01 (work in progress), October 2019.

[I-D.moskowitz-hip-new-crypto] Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", draft-moskowitz-hip-new-crypto-02 (work in progress), October 2019.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[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/info/rfc7401>.

Authors' Addresses

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
USA

Email: adam.wiethuechter@axenterprize.com

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
USA

Email: stu.card@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
USA

Email: rgm@labs.htt-consult.com