Workgroup: DRIP
Internet-Draft:
draft-wiethuechter-drip-auth-03
Published: 27 July 2020
Intended Status: Standards Track
Expires: 28 January 2021
A   A. Wiethuechter   S. Card   R. Moskowitz
        uAX Enterprize   AX Enterprize   HTT Consulting
        t
        h
        o
        r
        s
        :

DRIP Authentication Formats

Abstract

This document describes how to include trust into the ASTM Remote ID specification defined in ASTM 3411-19 under a Broadcast Remote ID (RID) scenario. It defines a few different message schemes (based on the Authentication Message) that can be used to assure past messages sent by a UA and also act as an assurance for UA trustworthiness in the absence of Internet connectivity at the receiving node.

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 28 January 2021.

Table of Contents

1. Introduction
  1.1. DRIP Requirements Addressed
2. Terms and Definitions
  2.1. Requirements Terminology
  2.2. Definitions
3. Background
  3.1. Problem Space And Document Focus
  3.2. ASTM Authentication Message
4. DRIP Authentication Framing Formats
  4.1. DRIP Authentication Frame
    4.1.1. DRIP Header
    4.1.2. DRIP Authentication Data
    4.1.3. Forward Error Correction
  4.2. DRIP Wrapper Frame
    4.2.1. UA Hierarchical Host Identity Tag
    4.2.2. Trust Timestamp
    4.2.3. Authentication Data
    4.2.4. Signature
5. Bluetooth 4.X Formats
  5.1. [1-4] Wrapped ASTM Message(s)
  5.2. 5 Wrapped ASTM Message(s)
  5.3. Manifest
    5.3.1. Hash Algorithm And Operation
    5.3.2. 4 Byte Manifest
    5.3.3. 8 Byte Manifest
    5.3.4. Pseudo-blockchain Hashes
    5.3.5. Limitations
  5.4. Certificate
  5.5. Recommendations
6. Bluetooth 5 Formats
  6.1. Certificate
  6.2. Message Pack Signature
7. Examples
  7.1. 2 Wrapped ASTM Messages
8. Security Considerations
9. ASTM Considerations
10. Acknowledgments
11. References
  11.1. Normative References
  11.2. Informative References
Appendix A. Thoughts on ASTM Authentication Message
Authors' Addresses

1. Introduction

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.

Observer systems (e.g. smartphones and tablets) place further constraints on the communication options. The Remote ID Broadcast messages MUST be available to applications on these platforms without modifying the devices.

The ASTM standard [F3411-19] focuses on two ways of communicating to a UAS for RID: Broadcast and Network.

This document will focus on adding trust to Broadcast RID in the Authentication Message format.

1.1. DRIP Requirements Addressed

The following [drip-requirements] will be addressed:

GEN 1: Provable Ownership
This will be addressed using the Certificate Message types (Section 5.4, Section 6.1).

GEN 2: Provable Binding
This will be addressed using the Wrapped ASTM Message, Manifest Message and Message Pack Signature types (Section 4.2, Section 5.3, Section 6.2).

GEN 3: Provable Registration
This will be addressed using the Certificate Message types (Section 5.4, Section 6.1).

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 [drip-requirements] for common DRIP terms.

Aircraft
In this document whenever the word Aircraft is used it is refering to an Unmanned Aircraft (UA) not a Manned Aircraft.

HI
Host Identity. The public key portion of an asymmetric keypair from HIP. In this document it is assumed that the HI is based on a EdDSA25519 keypair. This is supported by new crypto defined in [new-hip-crypto].

HIT
Host Identity Tag. A 128 bit handle on the HI. Defined in HIPv2 [RFC7401].

HHIT
Hierarchical Host Identity Tag. A 128 bit handle on the HI contain extra information not found in a standard HIT. Defined in [hierarchical-hit].

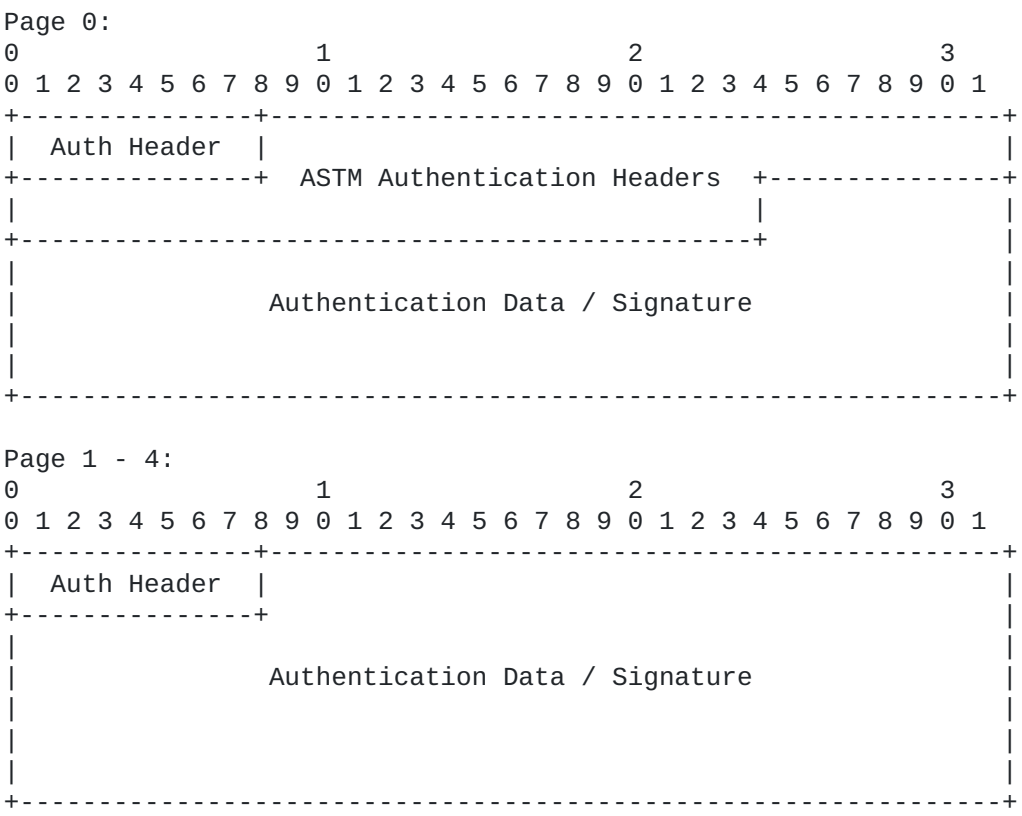
3. Background

3.1. Problem Space And Document Focus

The current 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.

The following subsections will provide a high level reference to the ASTM standard for Authentication Messages and how their current limitations effect trust in the Broadcast RID environment.

3.2. ASTM Authentication Message



Auth Header (1 byte):
Contains Authentication Type and Page Number. For DRIP Authentication this is a value of 0xD.

ASTM Authentication Headers: (6 bytes)
Contains other header information for the Authentication Message from ASTM UAS RID Standard.

Authentication Data / Signature: (109 bytes: 17+23*4)
Opaque authentication data.

The above diagram is the format defined by ASTM that is the frame which everything this document fits into. The specific details of

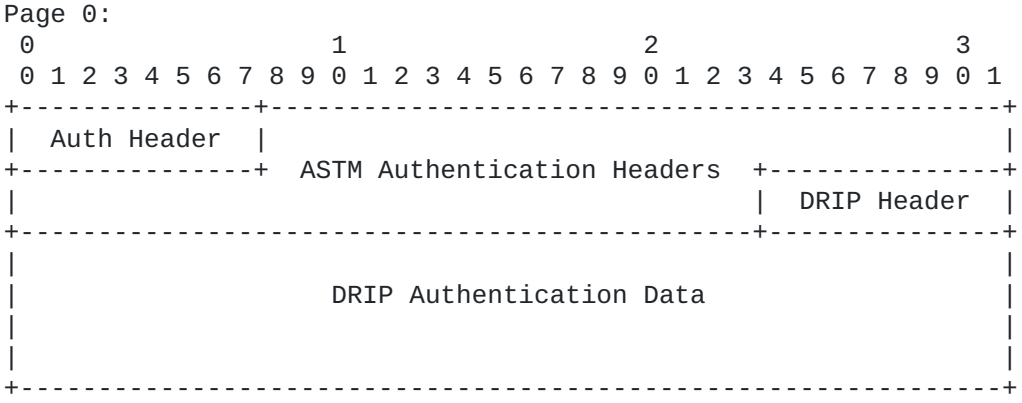
the ASTM headers are abstracted away as they are not necessarily required for this document.

4. DRIP Authentication Framing Formats

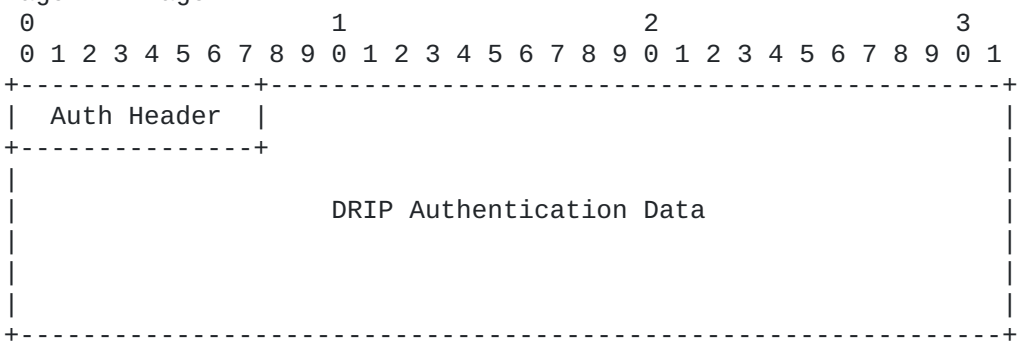
Currently the ASTM AuthType of 0xD should be used to denote DRIP based Authentication. The max page count of the Authentication Message is also 10, instead of 5.

4.1. DRIP Authentication Frame

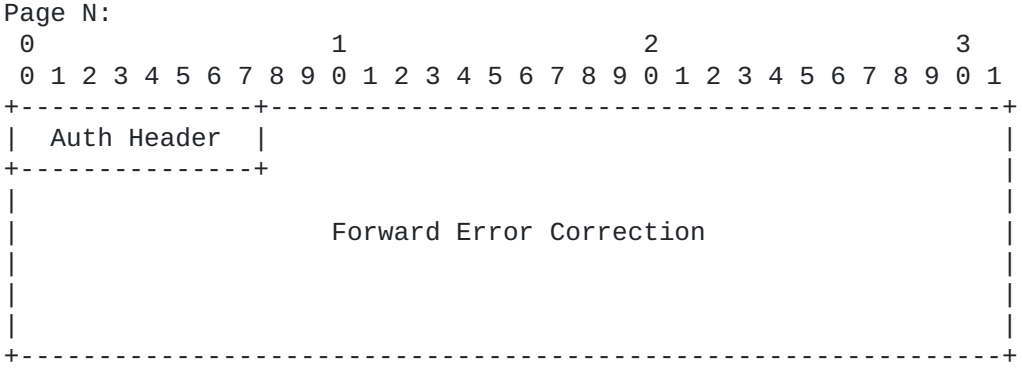
Page 0:



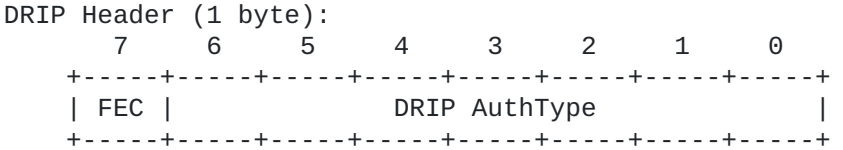
Page 1 - Page N-1:



Page N:



DRIP Header (1 byte):



FEC (1 bit):
Enabled [1] or Disabled [0]. Signals if Page N is filled with Reed Solomon FEC.

DRIP AuthType (7 bits):

DRIP AuthType	Values
0 Wrapped ASTM Message(s)	0
1 Wrapped ASTM Message(s)	1
2 Wrapped ASTM Message(s)	2
3 Wrapped ASTM Message(s)	3

4 Wrapped ASTM Message(s)	4
5 Wrapped ASTM Message(s)	5
8 Byte Manifest	6
4 Byte Manifest	7
Reserved (Wrapped Messages)	8-15
Certificate: Registry on Aircraft	16
Reserved (Certificates)	17-31
Private Use	32-63
Reserved	64-111
Experimental Use	112-127

DRIP Authentication Data (223 bytes):
    DRIP Authentication data. 0 to 223 bytes.

Forward Error Correction (23 bytes):
    Optional and signaled using DRIP Header. Always last
    Authentication page. Reed Solomon across preceding pages.

4.1.1. DRIP Header

The DRIP Header is used to signal what kind of Authentication under DRIP that the message is using and consists of two fields.

The Most Significant Bit is used to signal if FEC is present in the final page of the Authentication Message. It MUST be set to 1 if FEC is being used.

The lower 7 bits are used as the DRIP AuthType field denoting what Authentication type is being used. There are 5 major areas carved out of the DRIP AuthType defined by the following bitmaps:

```
 000 xxxx (0x00-0x0F): Wrapped Messages (16)
 001 xxxx (0x10-0x1F): Certificates (16)
 01x xxxx (0x20-0x3F): Private Use (32)
 1xx xxxx (0x40-0x6F): Reserved (48)
 111 xxxx (0x70-0x7F): Experimental Use (16)
```

4.1.2. DRIP Authentication Data

This field has a maximum size of 223 bytes. If the data is less than 223 bytes and a page is only partially filled then the rest of the partially filled page must be null padded.

4.1.3. Forward Error Correction

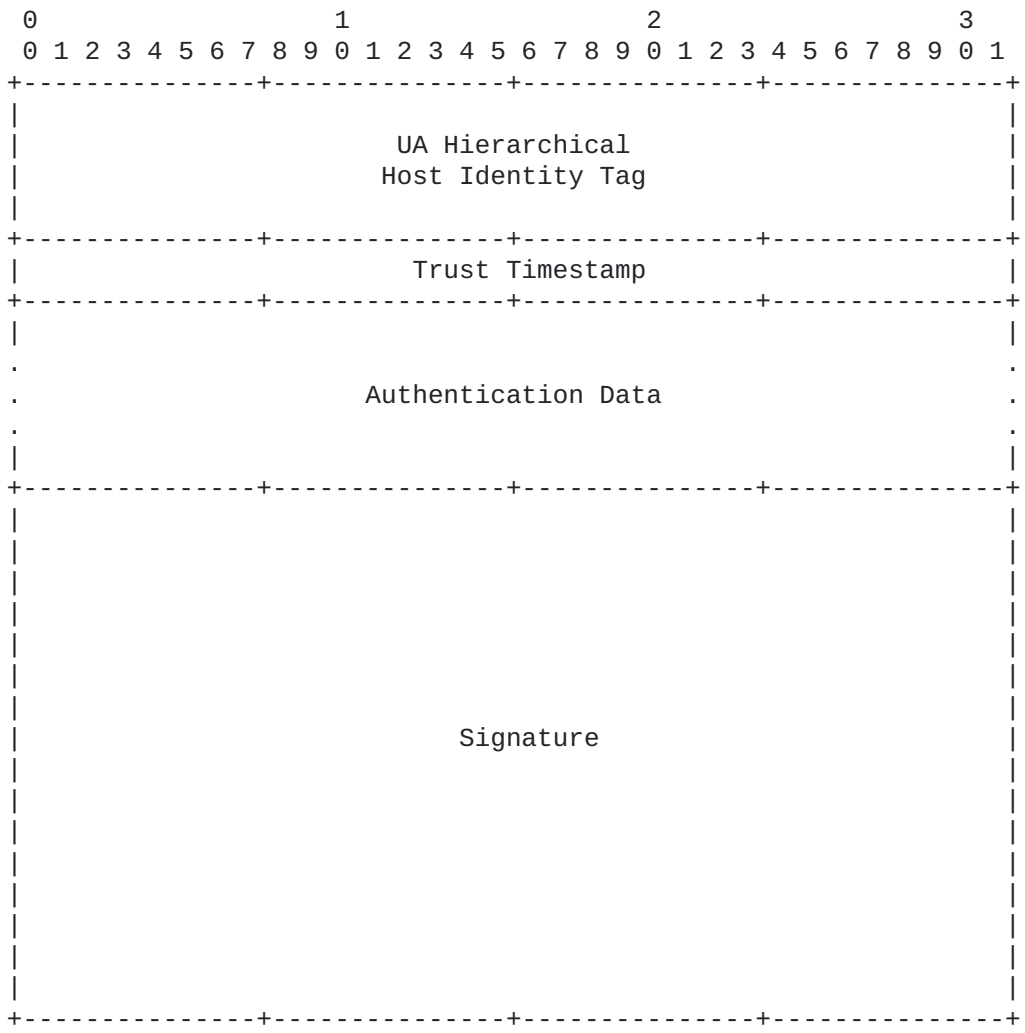
To help Bluetooth (specifically Bluetooth 4) achieve the goal of reliable receipt of paged messages a Forward Error Correction (FEC) scheme is introduced and SHOULD be used for Bluetooth 4 and SHOULD NOT be used for Bluetooth 5 under DRIP.

Due to the nature of Bluetooth 4 and the existing ASTM paging structure an optimization can be used. If a Bluetooth frame fails its CRC check, then the frame is dropped without notification to the upper protocol layers. From the Remote ID perspective this means the loss of a complete frame/message/page. In Authentication Messages, each page is already numbered so the loss of a page allows the receiving application to build a "dummy" page filled with nulls (other than the ASTM Header and Auth Header which is known).

A compliant implementation of this standard MUST use Reed Solomon for the FEC. With this the entire authentication message (all pages, including headers) are used to generate 23 bytes of parity. This parity is appended in one full page (always the last) allowing for recovery when any single page is lost in transmission.

If more than one page is lost (>1/5 for 5 page messages, >1/10 for 10 page messages) than the error rate of the link is already beyond saving and the application has more issues to deal with.

4.2. DRIP Wrapper Frame



UA Hierarchial Host Identity Tag (16 bytes):
    The UAs HHIT in byte form. Hashed from the EdDSA25519
    public key.

Trust Timestamp (4 bytes):
    Timestamp denoting current time plus an offset to trust
    message to.

Authentication Data (116/139 bytes):
    Opaque authentication data using DRIP format specified in
    the DRIP Header. 0 to 116 bytes when FEC bit is 1, 0 to
    139 bytes when FEC bit is 0.

Signature (64 bytes):
    Signature over preceding fields using the EdDSA25519
    keypair.

This framing resides within the General Frame's DRIP Authentication Data (Section 4.1.2).

4.2.1. UA Hierarchical Host Identity Tag

To avoid needing the UAs HHIT via the ASTM Basic ID in a detached fashion the 16 byte HHIT of the UA is included in the wrapper frame.

The HHIT for the UA (and other entities in the RID and greater UTM system under DRIP) is an enhancement of the Host Identity Tag (HIT) of HIPv2 [RFC7401] introducing hierarchy as defined in HHIT [hierarchical-hit].

Using Hierarchical HITs for UAS RID is outlined in HHIT based UAS RID [drip-uas-rid].

4.2.2. Trust Timestamp

Trust Timestamp MUST be current UNIX time plus an offset into the future. To avoid replay attacks the Trust Timestamp field must be well founded.

When wrapping a Vector (Position) Message the payload WILL contain (by ASTM rules) constantly changing data, this includes its own timestamp. This timestamp is only 2 bytes, which is easily attacked and only expresses the 1/10th of seconds since the last hour.

Other ASTM message types, such as Basic ID and Self-ID are static messages with no changing data. To protect a replay of these signed messages the Trust Timestamp is the field during signing to be guaranteed to change.

The offset used against the UNIX timestamp is not defined in this document. Best practices to identify a acceptable offset should be used taking into consideration the UA environment, and propagation characteristics of the messages being sent.

4.2.3. Authentication Data

This field has a maximum of 116 bytes in length when the FEC bit of the DRIP Header is turned on and 139 bytes of maximum length when turned off.

4.2.4. Signature

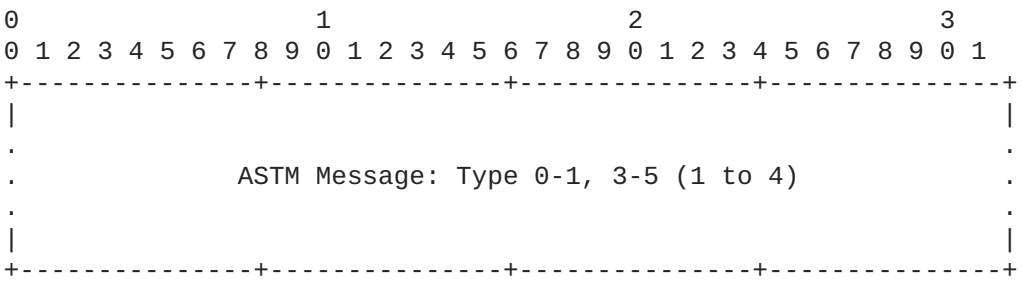
The wrapper signature is generated using the private key half of the the UAs Host Identity (HI) and is done over all preceding data. ASTM/DRIP Headers are exclude from this operation only information within the DRIP Wrapper Frame is signed.

5. Bluetooth 4.X Formats

With Bluetooth 4.X formatting the goal is to attempt to bring reliable receipt of paged messages.

Unless otherwise specified the FEC Bit of the DRIP Header MUST be set to 1 when using Bluetooth 4 to take advantage of FEC for lost frames.

5.1. [1-4] Wrapped ASTM Message(s)



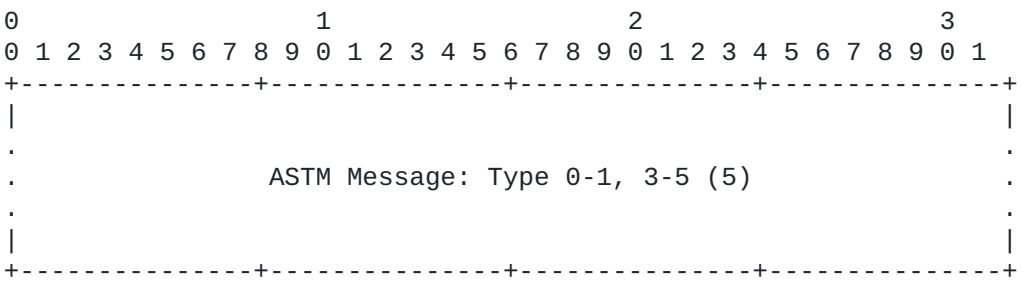
DRIP Header:
    With FEC: 0x81-0x84 [129-132] (RECOMMENDED)
    Without FEC: 0x01-0x04 [1-4]

ASTM Message: Type 0-1, 3-5 (25 bytes):
    Valid ASTM Messages of Type 0, 1, 3, 4, or 5.
    If more than 1 then ASTM Messages in Message Type order.

This DRIP Authentication type uses the Wrapper Frame format (Section 4.2), filling the Authentication Data (Section 4.2.3) field with an ASTM Message (all types except Message Pack [0xF] and Authentication [0x2]).

When multiple ASTM Messages are being wrapped they MUST be in Message Type order.

5.2. 5 Wrapped ASTM Message(s)



DRIP Header:
    With FEC: 0x85 [133] (RECOMMENDED)
    Without FEC: 0x05 [5]

ASTM Message: Type 0-1, 3-5 (25 bytes):
    5 valid ASTM Message of Types 0, 1, 3, 4, or 5.
    ASTM Messages in Message Type order.

This DRIP Authentication type uses the Wrapper Frame format (Section 4.2), filling the Authentication Data (Section 4.2.3) field with an ASTM Message (all types except Message Pack [0xF] and Authentication [0x2]).

ASTM Messages being wrapped MUST be in Message Type order.

5.3. Manifest

This DRIP Authentication type uses the Wrapper Frame format (Section 4.2), filling the Authentication Data (Section 4.2.3) field with hashes of previously sent messages.

By hashing previously sent messages and signing them we gain trust in UAs 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.

5.3.1. Hash Algorithm And Operation

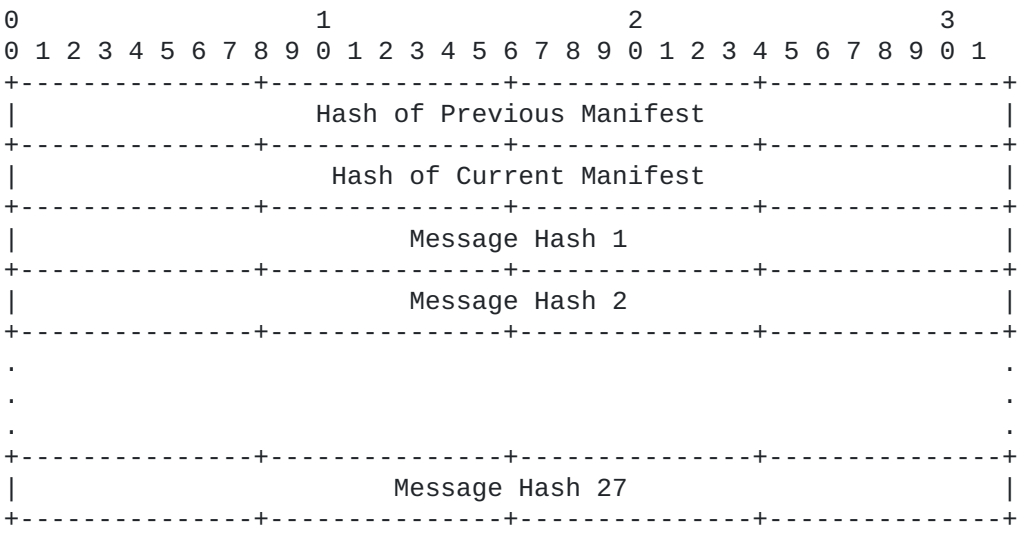
The hash algorithm used for the Manifest Message is the same hash algorithm used in creation of the HHIT that is signing the Manifest.

A standard HHIT would be using cSHAKE128 from [NIST.SP.800-185]. With cSHAKE128, the hash is computed as follows:

```
cSHAKE128(MAC|Message, 8*H-Len, "", "RemoteID Auth Hash")
```

The message MAC is prepended to the message, as the MAC is the only information that links UA messages from a specific UA.

5.3.2. 4 Byte Manifest



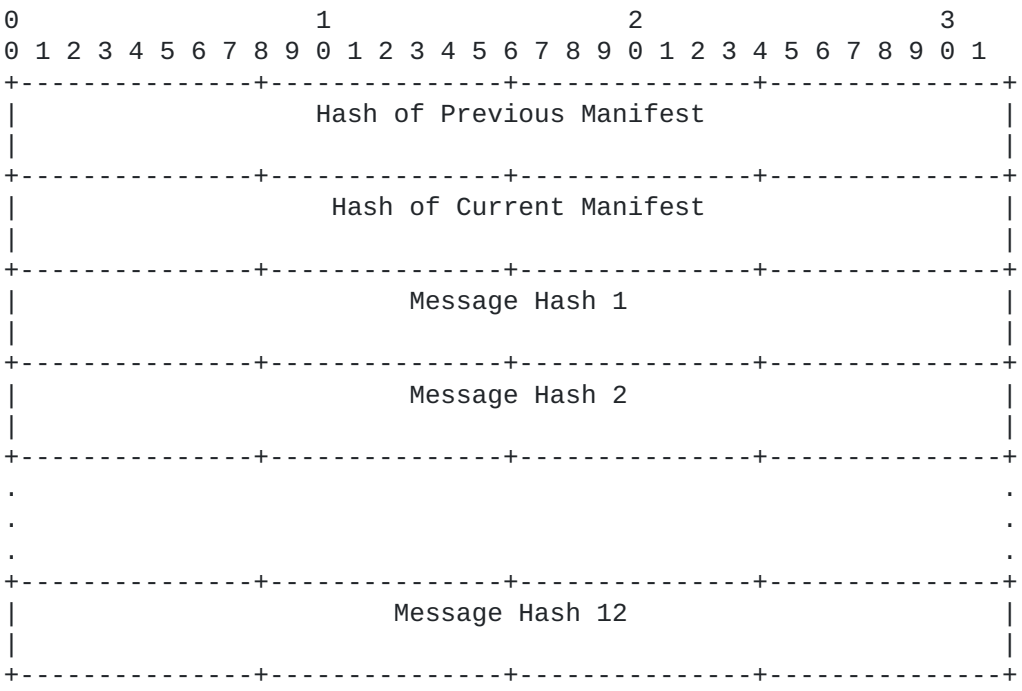
DRIP Header:
    With FEC: 0x86 [132] (RECOMMENDED)
    Without FEC: 0x06 [6]

Hash of Previous Manifest: (4 bytes)
    A hash of the previously sent Authentication message.

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

Message Hash: (4 bytes)
    A hash of a previously sent message. 27 max.

5.3.3. 8 Byte Manifest



DRIP Header:
    With FEC: 0x87 [135] (RECOMMENDED)
    Without FEC: 0x07 [7]

Hash of Previous Manifest: (8 bytes)
    A hash of the previously sent Authentication message.

Hash of Current Manifest: (8 bytes)
    A hash of the current Authentication message.

Message Hash: (8 bytes)
    A hash of a previously sent message. 12 max.

5.3.4. Pseudo-blockchain Hashes

Two special hashes are included; a previous manifest hash, which links to the previous manifest message, as well as a current manifest hash. This gives a pseudo-blockchain provenance to the manifest 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 manifest hash field:

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.

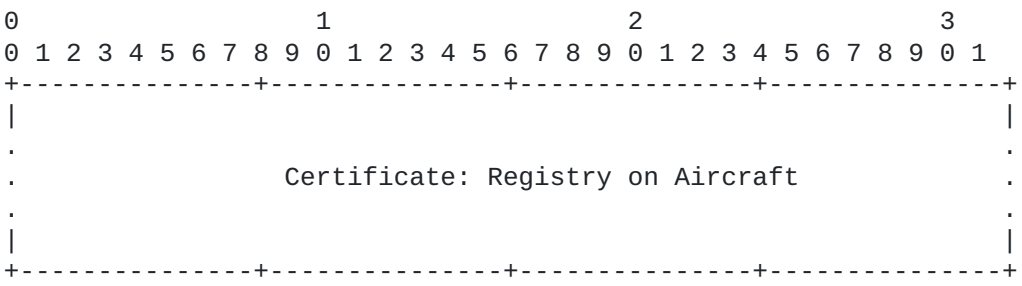
There a few different ways to cycle this message. We can "roll up" the hash of 'current' to 'previous' when needed or to

completely recompute the hash. This mostly depends on the previous note.

5.3.5. Limitations

A potential limitation to this format is dwell time of the UA. If the UA is not sticking to a general area then most likely the Observer will not obtain many (if not all) of the messages in the manifest. Without the original messages received no verification can be done. Examples of such scenarios include delivery or survey UA.

5.4. Certificate



DRIP Header:
With FEC: 0x90 [144] (RECOMMENDED)
Without FEC: 0x10 [16]

Certificate: Registry on Aircraft (200 bytes):
A certificate granted by the Registry that asserts the binding of UA to the given Registry.

This DRIP Authentication type uses the General Frame format (Section 4.1), filling the DRIP Authentication Data (Section 4.1.2) field with a 200 byte Certificate: Registry on Aircraft.

What this grants is the ability to authenticate UA Remote ID when the receiving device of the observer (e.g. a smartphone with a dedicated RID application) has no Internet service (e.g. LTE signal).

The Certificate: Registry on Aircraft (Cra) is in practice a binding claim between the Registry and the Aircraft, asserting the relationship between the two entities. Cra signs another certificate, Caa (Certificate: Aircraft on Aircraft), that is created during UA provisioning.

Importantly this certificate allows offline signature verification from the UA. This is as the UA HI is included in the certificate. Also included is the HHIT of the Registry to check the local shortlist of Registries that the Observer device trusts (mapping HHITs to HIs).

More details about Caa, Cra, other certificates and the provisioning process can be found in [drip-identity-claims].

5.5. Recommendations

Under ASTM Bluetooth 4.X rules, transmission of dynamic messages are at least every 1 second while static messages (which is what Authentication is classified under) are sent at least every 3 seconds.

Under DRIP the Certificate Message MUST be transmitted to properly meet the GEN 1 and GEN 3 requirement.

The ASTM Message Wrapper and Manifest both satisfy the GEN 2 requirement. At least one MUST be implemented to comply with the GEN 2 requirement.

A single Manifest can carry at most (using the full 10 page limit and 8 byte hashes) 12 unique hashes of previously sent messages (of any type). This results in a total of 22 (12 + 10) frames of Bluetooth data being transmitted over Bluetooth.

In comparison the Message Wrapper sends 6 pages (each a single frame) for each wrapped message. For backwards compatibility the implementation should also send the standard ASTM message that was wrapped for non-DRIP compliant receivers to obtain. This method results in 84 total Bluetooth frames (12 + (12 * 6)) sent.

The question of which is better suited is up to the implementation.

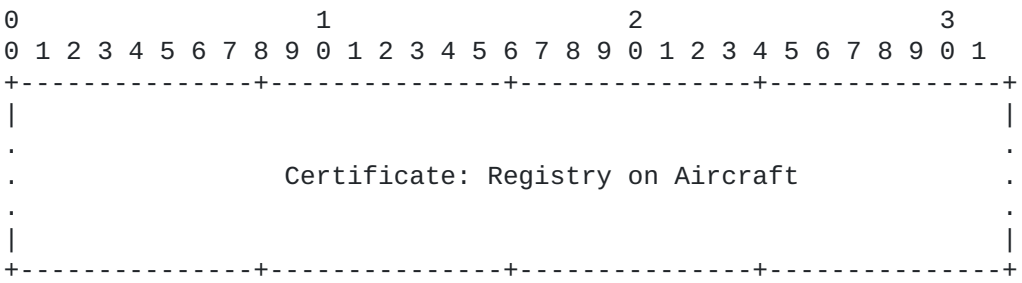
6. Bluetooth 5 Formats

Under ASTM specification, Bluetooth 5 transport of Remote ID is to use the Message Pack (Type 0xF) format for all transmissions. Under Message Pack all messages are sent together (in Message Type order) in a single Bluetooth frame (up to 250 bytes). Message Packs are required by ASTM to be sent at a rate of 1 per second (like dynamic messages).

This gives the benefit of no longer is there any message or page fragmentation in transmission. For this reason the recommended use of FEC such as Reed Solomon using in Bluetooth 4.X is not needed here and is impractical.

Any of the Bluetooth 4.X formats can theoretically be used during Bluetooth 5 operation under ASTM, however the following subsections define a number of formats optimized for Message Pack and Bluetooth 5.

6.1. Certificate

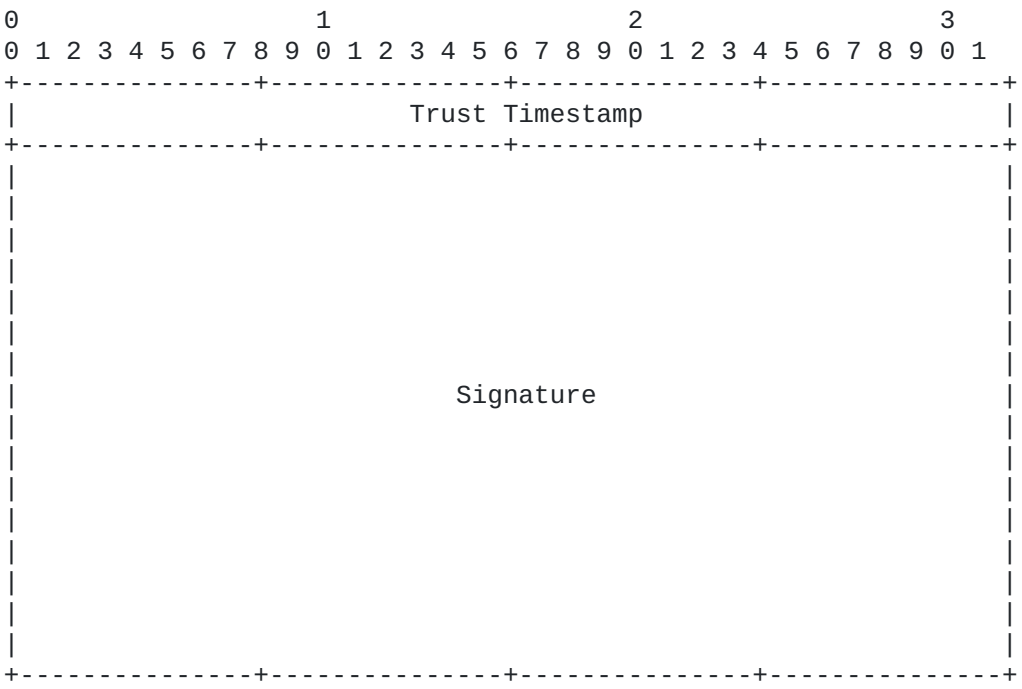


DRIP Header:
    With FEC: 0x90 [144]
    Without FEC: 0x10 [16] (RECOMMENDED)

Certificate: Registry on Aircraft (200 bytes):
    A certificate granted by the Registry that asserts the
    binding of UA to the given Registry.

With Message Pack the following SHOULD be included in it when sending a DRIP Certificate Message: 1x Location Message 1x Authentication Message, DRIP AuthType 16 The Certificate Message (without FEC) only needs 9 pages for transmission, allowing the final 25 bytes to be used for another ASTM Message.

6.2. Message Pack Signature



Trust Timestamp: (4 bytes)
    Timestamp denoting current time plus an offset to trust
    message to.

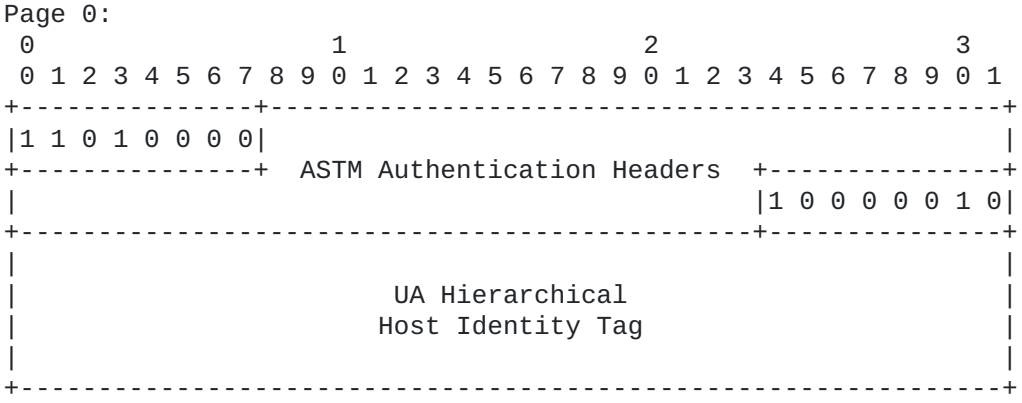
Signature: (64 bytes)
    Signature over all messages in Message Pack using the
    EdDSA25519 keypair.

The DRIP Message Pack Signature is a DRIP AuthType 0. All messages in the message pack (excluding the Authentication Message itself) is signed.

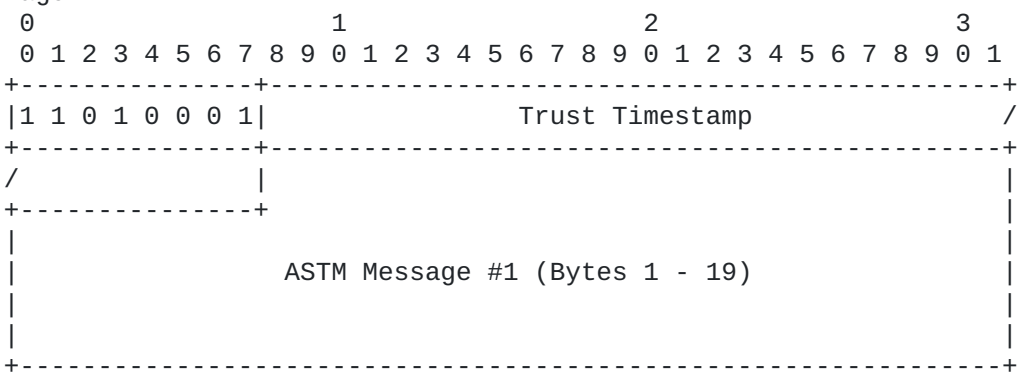
7. Examples

7.1. 2 Wrapped ASTM Messages

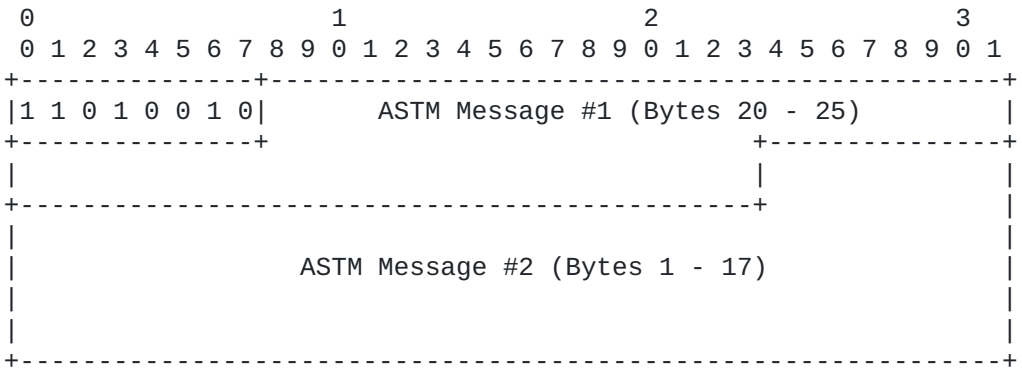
Page 0:



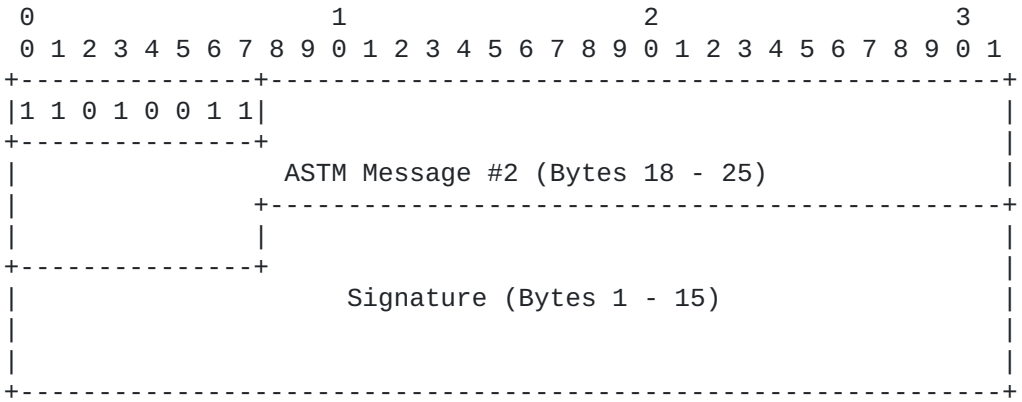
Page 1:



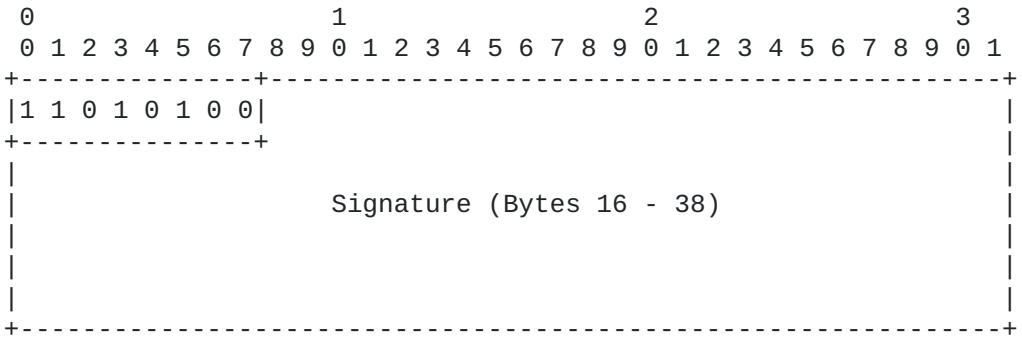
Page 2:



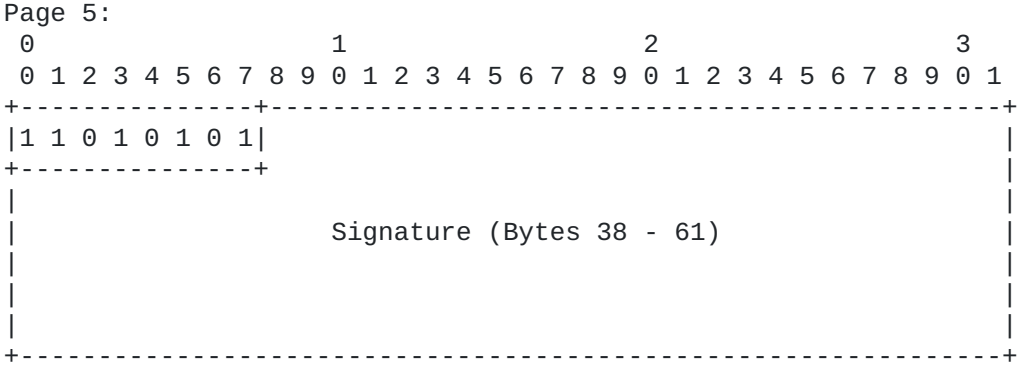
Page 3:



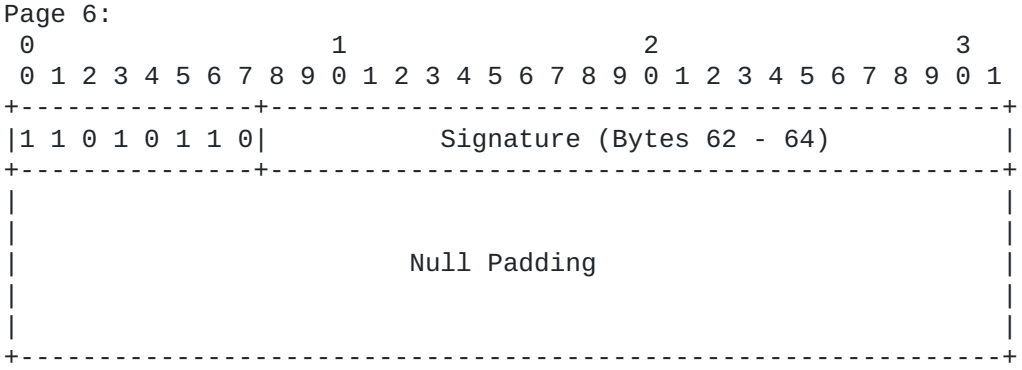
Page 4:



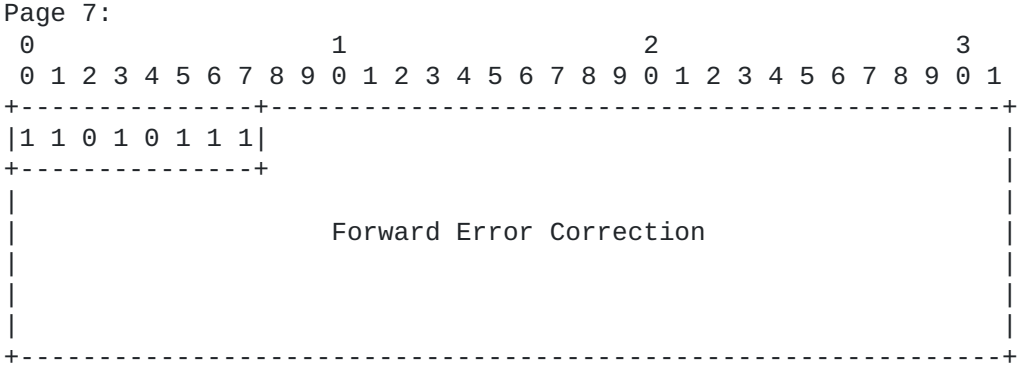
Page 5:



Page 6:



Page 7:



8. Security Considerations

TBD

9. ASTM Considerations

1. Increase Authentication Page Count maximum from 5 to 10.

2. Add Authentication Type for DRIP.

10. Acknowledgments

Ryan Quigley and James Mussi at AX Enterprize for early prototyping to find holes in the draft specifications.

11. References

11.1. Normative References

[NIST.SP.800-185] Kelsey, J., Change, S., and R. Perlner, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[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>.

11.2. Informative References

[drip-identity-claims] Wiethuechter, A., Card, S., and R. Moskowitz, "DRIP Identity Claims", Work in Progress, Internet-Draft, draft-wiethuechter-drip-identity-claims-00, 23 March 2020, <https://tools.ietf.org/html/draft-wiethuechter-drip-identity-claims-00>.

[drip-requirements] Card, S., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements", Work in Progress, Internet-Draft, draft-ietf-drip-reqs-03, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-drip-reqs-03>.

[drip-uas-rid] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "UAS Remote ID", Work in Progress, Internet-Draft, draft-moskowitz-drip-uas-rid-03, 13 July 2020, <https://tools.ietf.org/html/draft-moskowitz-drip-uas-rid-03>.

[F3411-19] ASTM International, "Standard Specification for Remote ID and Tracking", February 2020, <http://www.astm.org/cgi-bin/resolver.cgi?F3411>.

[hierarchical-hit]
Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", Work in Progress, Internet-Draft, draft-moskowitz-hip-hierarchical-hit-05, 13 May 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-hierarchical-hit-05>.

[new-hip-crypto] Moskowitz, R., Card, S., and A. Wiethuechter, "New Cryptographic Algorithms for HIP", Work in Progress, Internet-Draft, draft-moskowitz-hip-new-crypto-04, 23 January 2020, <https://tools.ietf.org/html/draft-moskowitz-hip-new-crypto-04>.

[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>.

Appendix A. Thoughts on ASTM Authentication Message

The format standardized by the ASTM is designed with a few major considerations in mind, which the authors of this document feel put significant limitations on the expansion of the standard.

The primary consideration (in this context) is the use of the Bluetooth 5.X Extended Frame format. This method allows for a 255 byte payload to be sent in what the ASTM refers to as a "Message Pack".

The idea is to include up to five standard ASTM Broadcast RID messages (each of which are 25 bytes) plus a single authentication message (5 pages of 25 bytes each) in the Message Pack. The reasoning is then the Authentication Message is for the entire Message Pack.

The authors have no issues with this proposed approach; this is a valid format to use for the Authentication Message provided by the ASTM. However, by limiting the Authentication Message to ONLY five pages in the standard it ignores the possibility of other formatting options to be created and used.

Another issue with this format, not fully addressed in this document is fragmentation. Under Bluetooth 4.X, each page is sent separately which can result in lose of pages on the receiver. This is disastrous as the loss of even a single page means any signature is incomplete.

With the current limitation of 5 pages, Forward Error Correction (FEC) is nearly impossible without sacrificing the amount of data sent. More pages would allow FEC to be performed on the Authentication Message pages so loss of pages can be mitigated.

All these problems are further amplified by the speed at which UA fly and the Observer's position to receive transmissions. There is no guarantee that the Observer will receive all the pages of even a 5 page Authentication Message in the time it takes a UA to traverse across their line of sight. Worse still is that is not including other UA in the area, which congests the spectrum and could cause

further confusion attempting to collate messages from various UA. This specific problem is out of scope for this document and our solutions in general, but should be noted as a design consideration.

Authors' Addresses

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

Email: adam.wiethuechter@axenterprize.com

Stuart W. Card
AX Enterprize
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