TMRID
Internet-Draft
Intended status: Standards Track
Expires: 3 May 2020

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

TM-RID Authentication Formats
draft-wiethuechter-tmrid-auth-03

Abstract

This document describes how to include trust 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 (based on the authentication message) 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.

Status of This Memo

Copyright Notice

Table of Contents

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 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 current authentication message format, using the Host Identity Protocol Version 2 (HIPv2) [RFC7401] Hierarchical HIT (HHIT) [I-D.moskowitz-hip-hierarchical-hit].

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. A set of organizational and technical attributes and processes that employs human, physical, and information resources to solve problems and accomplish missions. Mainly used in military contexts.

HI
: Host Identity. The public key portion of an assymetric 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 [I-D.moskowitz-hip-new-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 [I-D.moskowitz-hip-hierarchical-hit].

UA
: Unmanned Aircraft. In this document UA's are typically though of as drones of commerical or military variety. This is a very strict definition which can be relaxed to include any and all aircraft that are unmanned.

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 C2 links between UA and the control station.

UTM — UAS Traffic Management. A "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management (ATM) system.

USS — UAS Service Supplier. 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).

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

Observer — Referred to in other UAS documents as a "user", but there are also other classes of RID users, so we prefer "observer" to denote an individual who has observed an UA and wishes to know something about it, starting with its RID.

3. Background

3.1. Problem Space And Document Focus

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.

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 envirorment.

3.2. ASTM Authentication Message

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
+---------------------------------------------------------------+
|                                                               |
|            ASTM UAS RID HEADERS              +---------------+
|                                              |               |
+----------------------------------------------+               |
|                                                               |
|                                                               |
|                                                               |
|                Authentication Data / Signature                |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+
```

Page 1 - 4:

```
 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
+---------------+-----------------------------------------------+
|  ASTM HEADER  |                                               |
+---------------+                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                 Authentication Data / Signature               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+
```

ASTM UAS RID Headers: (7 bytes)
    Contains header information for the authentication message from ASTM UAS RID Standard.
    A short 1 byte header is also present as ASTM HEADER included on every page.

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

3.3. Thoughts on ASTM Authentication Message

The format proposed by the ASTM is designed with a few major considerations in mind, which the authors 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 an "atomic message".

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 an atomic message. The reasoning is then the authentication message is for the entire atomic 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.

3.4. TM-RID Supporting Levels

This document is assuming that the first two levels of TM-RID (Identification and Authentication) are implemented. This document serves as a expansion to these two levels, leveraging the abilities of the HHIT Registries [I-D.moskowitz-hip-hhit-registries] to its fullest potential.

4. 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.

4.1. HIP Based Authentication Wrapper

```
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
+---------------------------------------------------------------+
|                                                               |
|            ASTM UAS RID HEADERS              +---------------+
|                                              |    RESERVED   |
+----------------------------------------------+---------------+
|                                                               |
|                                                               |
|                                                               |
|                            HHIT                               |
|                                                               |
|                                                               |
```

```
   |                                                               |
   +---------------------------------------------------------------+

   Page 1:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                 Trust Timestamp               /
   +---------------+---------------+-------------------------------+
   /               |    RESERVED   |                               |
   +---------------+---------------+                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                          HHIT Signature                       |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 2:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                          HHIT Signature                       |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 3:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                          HHIT Signature                       |
```

```
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+
```

Page 4:

```
 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
+---------------+-----------------------------------------------+
|  ASTM HEADER  |                                               |
+---------------+                                               |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
|                            Payload                            |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
+---------------------------------------------------------------+
```

HHIT: (16 bytes)
    HHIT using the EdDSA25519 HI.

Trust Timestamp: (4 bytes)
    Timestamp denoting a future time to trust message to.

HHIT Signature: (64 bytes)
    Signature of payload using the EdDSA25519 keypair.
    Spread across 3 pages.

Payload: (0 to 23/25 bytes)
    Opaque payload data that has been used in signing.
    This can be increased to 25 by removing padding RESERVED
    sections.

This format is a way to authenticate a given UA using Level 1 and Level 2 of the TM-RID architecture.

When this authentication format is recieved the HHIT (provided by Level 1 TM-RID) is first looked up by mechanisms defined in Level 2. This lookup chain ultimately obtains, on the Observers device, the full HI associated with the HHIT recieved. Once completed the signature can then be verifed with the respective data it was signed with. This data, at a minimum would be the payload in the authentication message.

The payload can be anything that fits within the 23/25 byte limit. Some examples of what could be done with this format are found in Section 5.

4.2. Signed Hash Lists

```
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
+---------------------------------------------------------------+
|                                                               |
|            ASTM UAS RID HEADERS               +---------------+
|                                               | H-Alg | H-Len |
+---------------------------------------------------------------+
|                Hash of Previous Auth. Message                 |
+---------------------------------------------------------------+
|                Hash of Current Auth. Message                  |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+

DataPage 1:
 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
+---------------+---------------+-------------------------------+
|  ASTM HEADER  | H-Alg | H-Len |            RESERVED           |
+---------------+---------------+-------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+
|                          Message Hash                         |
+---------------------------------------------------------------+

Page 2:
 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
+---------------+---------------+-------------------------------+
|  ASTM HEADER  |    RESERVED   |       Signature Length        |
+---------------+---------------+-------------------------------+
|       Signature Algorithm     |                               |
+-------------------------------+                               |
```

```
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 3:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 4:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+
```

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.

```
H-Alg       Values
-----       ------
RESERVED    0
cSHAKE128   1 [sp800-185] (RECOMMENDED)
```

Hash of Previous Auth. Message: (4 bytes)
A hash of the previously sent 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 HI from HIP.
Spread across 3 pages.

This format is designed to provide provenance to Broadcast RID messages sent by a given UAS. It should be noted that the HHIT is not provided in the format like others specified here - instead it must be obtained via the Basic ID Message in a detached fashion.

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.

4.2.1. Hash Operation

With cSHAKE128 NIST SP 800-185 [NIST.SP.800-185], 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 a UA's messages from a specific UA.

4.2.2. Pseudo-blockchain 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:

> 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.

4.2.3. Limitations

With the current format proposed by ASTM only 7 messages can be hashed reasonably in the above format. RESERVED padding, the Signature Algorithm, Signature Length and redundant H-Alg, H-Len fields could be removed. This would increase the total list of hashes to 9 while losing word alignment of the hashes in each page.

To address this problem properly the authors feel that the Authentication Messages needs to have a max bound of 10 pages, instead of 5.

4.3. HIP Based Offline Authentication

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                            DEV HHIT                           |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            TIMESTAMP                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                            DEV HHIT                           |
|                              SIG                              |
```

```
   .                                                               .
   .                                                               .
   .                                                               .
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                              DEV HI                           |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         AUTH TIMESTAMP                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                           AUTH HHIT                           |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                            AUTH                               |
   |                              SIG                              |
   .                                                               .
   .                                                               .
   .                                                               .
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   /                            PAYLOAD                            /
   /                                                               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
   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
```

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.

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 UA without requiring the need for immediate reverse lookups online.

5. Example Use Cases

This section introduces potentional use cases of the HIP based extensions to the proposed ASTM standard authentication message.

5.1. Trusted Messages

Using the HIP Based Authentication Wrapper any single Broadcast RID message defined by ASTM can become what the authors refer to as a "Trusted Message".

One specific use case that is useful in the UAS RID space is the creation of a "Trusted Vector Message". By placing a previous [or new] vector message into the Payload section of this format 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 near real time.

The figure below is a example of a "Trusted Vector Message". Note that the padding (RESERVED) byte are now gone. The "Trust Timestamp" and "Vector Message" fields now span multiple pages instead of being aligned to pages.

```
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
+---------------------------------------------------------------+
|                                                               |
|            ASTM UAS RID HEADERS              +---------------+
|                                              |               |
+----------------------------------------------+               |
|                                                               |
|                                                               |
|                                                               |
|                              HHIT                             |
|                                                               |
|                                              +---------------+
|                                              |               /
```

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

   Page 1:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  /                 Trust Timestamp               |
   +---------------+-----------------------------------------------+
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 2:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 3:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         HHIT Signature                        |
   |                                                               |
   |                                                               |
```

```
   |                                                               |
   |                               +-------------------------------+
   |                               |        Vector Message         /
   +-------------------------------+-------------------------------+

   Page 4:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  /                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                         Vector Message                        |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+
```

5.2. Wrapped Signed Hashes

Using the HIP Based Authentication Wrapper a [short] list of hashes can be signed. These hashes are of previous individual RID messages.

This follows the format of the Signed Hash List, excluding the psuedo-blockchain hashes and various other fields enabling it to fit within the 23 byte limit of the final page.

To the authors, this format has limited use due to numerous concerns of replay attacks. It is suggested to instead use the full Signed Hash List format.

```
   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
   +---------------------------------------------------------------+
   |                                                               |
   |            ASTM UAS RID HEADERS               +---------------+
   |                                               |    RESERVED   |
   +-----------------------------------------------+---------------+
   |                                                               |
   |                                                               |
   |                                                               |
   |                             HHIT                              |
   |                                                               |
```

```
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 1:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                Trust Timestamp                /
   +---------------+---------------+-------------------------------+
   /               |    RESERVED   |                               |
   +---------------+---------------+                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                          HHIT Signature                       |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 2:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                          HHIT Signature                       |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   +---------------------------------------------------------------+

   Page 3:
    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
   +---------------+-----------------------------------------------+
   |  ASTM HEADER  |                                               |
   +---------------+                                               |
   |                                                               |
   |                                                               |
   |                                                               |
   |                                                               |
```

```
|                          HHIT Signature                           |
|                                                                   |
|                                                                   |
|                                                                   |
|                                                                   |
+-------------------------------------------------------------------+

Page 4:
 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
+----------------+----------------+---------------------------------+
|  ASTM HEADER   | H-Alg | H-Len |             RESERVED            |
+----------------+----------------+---------------------------------+
|                           Message Hash                            |
+-------------------------------------------------------------------+
|                           Message Hash                            |
+-------------------------------------------------------------------+
|                           Message Hash                            |
+-------------------------------------------------------------------+
|                           Message Hash                            |
+-------------------------------------------------------------------+
|                           Message Hash                            |
+-------------------------------------------------------------------+
```

6. IANA Considerations

TBD

7. Security Considerations

TBD

8. Acknowledgments

TBD

9. References

9.1. Normative References

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

9.2. 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), 17 October 2019, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-hhit-registries-01.txt>.

[I-D.moskowitz-hip-hierarchical-hit] Moskowitz, R., Card, S., and A. Wiethuechter, "Hierarchical HITs for HIPv2", draft-moskowitz-hip-hierarchical-hit-02 (work in progress), 17 October 2019, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-hierarchical-hit-02.txt>.

[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), 3 October 2019, <http://www.ietf.org/internet-drafts/draft-moskowitz-hip-new-crypto-02.txt>.

[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
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
0000
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com