

# DRIP Authentication Formats for Broadcast Remote ID

draft-ietf-drip-auth-03

Adam Wiethuechter (AX Enterprize, LLC), Etal.

# Changes since -01

- General
  - New title
  - Rearranged sections for clarity
  - Removal of specific F3411 reference (F3411-19 to F3411)
- Updated Section 3.3
- Reordering and expanded DRIP Auth. Formats
- Operational Recommendations added
- Appendices updates

1. Introduction	3
1.1. DRIP Requirements Addressed	3
2. Terminology	4
2.1. Required Terminology	4
2.2. Definitions	4
3. Background	4
3.1. Problem Space and Focus	4
3.2. Reasoning for IETF DRIP Authentication	4
3.3. ASTM Authentication Message	5
4. DRIP Authentication Formats	6
4.1. UAS ID Signature	6
4.2. Operator ID Signature	7
4.3. Message Set Signature	8
4.4. Specific Method	9
4.4.1. DRIP Frame Format	9
4.4.2. DRIP Wrapper Format	11
4.4.3. DRIP Manifest Format	11
4.4.4. DRIP Link Format	13
5. Transport Methods & Recommendations	13
5.1. Legacy Advertisements (Bluetooth 4.X)	13
5.2. Extended Advertisements (Bluetooth 5.X, WiFi NAN, WiFi Beacon)	14
5.3. DRIP Recommendations	14
6. ICAO Considerations	14
7. IANA Considerations	14
8. Security Considerations	14
8.1. Manifest Hash Length	15
8.2. Replay Attacks	15
8.3. Trust Timestamp Offsets	16
9. Acknowledgments	16
10. Appendix A: Thoughts on ASTM Authentication Message	16
11. Appendix B: DRIP Attestations	17
11.1. Self-Attestation (Axx)	17
11.2. Attestation (Axy)	18
11.3. Concise Attestation (C-Axy)	19
11.4. Mutual Attestation (M-Axy)	20
11.5. Link Attestation (L-Axy)	21
11.6. Broadcast Attestation (B-Axy)	22
11.7. Link Certificate (L-Cxy)	24
11.8. Mutual Certificate (M-Cxy)	24
11.9. Example Registration with Attestation	25
12. Appendix C: DRIP Broadcast Attestation Structure	26
12.1. Attestor Hierarchical Host Identity Tag	27
12.2. Attestation Data	27
12.3. Trust Timestamp	27
12.4. Signing Timestamp	27
12.5. Attestor Signature	28
13. Appendix D: Forward Error Correction	28
13.1. Encoding	28
13.1.1. Single Page FEC	28
13.1.2. Multi Page FEC	29
13.2. Decoding	29
13.2.1. Single Page FEC	29
13.2.2. Multi Page FEC	29
13.3. FEC Limitations	29
14. References	29
14.1. Normative References	29
14.2. Informative References	30
Authors' Addresses	30

1. Introduction	3
1.1. DRIP Requirements Addressed	3
2. Terminology	4
2.1. Required Terminology	4
2.2. Definitions	4
3. Background	4
3.1. Problem Space and Focus	4
3.2. Reasoning for IETF DRIP Authentication	4
3.3. ASTM Authentication Message	5
3.3.1. Authentication Page	5
3.3.2. DRIP Constraints	8
4. Forward Error Correction	8
4.1. Encoding	8
4.1.1. Single Page FEC	8
4.1.2. Multi Page FEC	8
4.2. Decoding	9
4.2.1. Single Page FEC	9
4.2.2. Multi Page FEC	9
4.3. FEC Limitations	9
5. Broadcast Attestation Structure	10
6. DRIP Authentication Formats	12
6.1. Operator ID Signature	12
6.2. Message Set Signature	13
6.3. Specific Authentication Method	14
6.3.1. SAM Data Format	15
6.3.2. DRIP Link	16
6.3.3. DRIP Wrapper	18
6.3.4. DRIP Manifest	20
6.3.5. DRIP Frame	23
7. Requirements & Recommendations	25
7.1. Legacy Transports	25
7.2. Extended Transports	25
7.3. Authentication	25
7.4. Operational	26
7.4.1. DRIP Wrapper	27
8. ICAO Considerations	27
9. IANA Considerations	27
10. Security Considerations	27
10.1. Manifest Hash Length	27
10.2. Replay Attacks	28
10.3. Trust Timestamp Offsets	29
11. Acknowledgments	29
12. References	29
12.1. Normative References	29
12.2. Informative References	30
Appendix A. Authentication Coloring Scheme	30
Appendix B. Example Authentication Messages	31
B.1. Authentication Data Only	31
B.2. Authentication Data & Additional Data	32
B.3. DRIP Link Example	34
Authors' Addresses	36

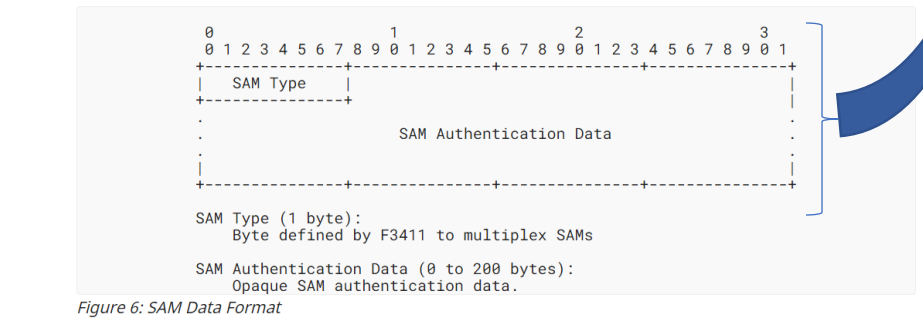
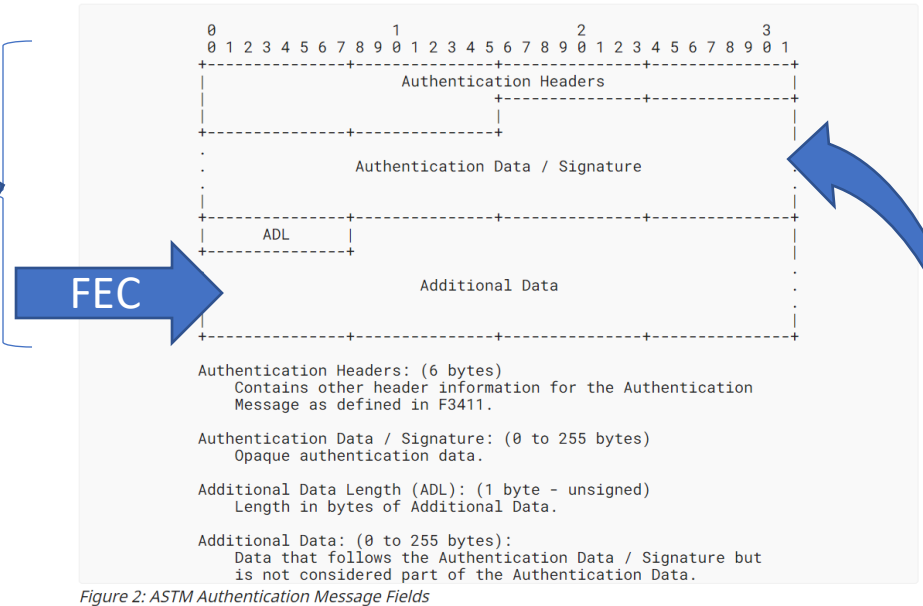
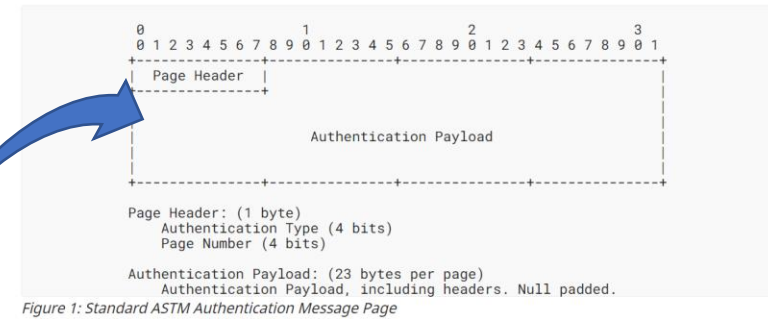
# Section 3.3 Rework

- The overview of "current" ASTM Authentication Message
  - Massive rework to make clearer but remain abstract
- Updated to F3411-v1.1 changes
  - Authentication Type 5 – Specific Authentication Methods (SAM)
  - Additional Data Length & Additional Data
- New DRIP Constraints section (3.3.2)
  - Sets up specific DRIP based constraints on the Authentication Message
- F3411-v1.1 re-balloting later this year (will become F3411-22?)

# F3411-v1.1 Changes

- Authentication Type 5 – SAM
  - Means to add Authentication formats to F3411 after publication
  - Single multiplexing byte (SAM Type) at start of Authentication Data
    - Maintained by ICAO
    - WG will need to submit request for values
- Additional Data Length (ADL) & Additional Data
  - Pseudo-field of data after Authentication Data
  - 16-pages of data = 362-bytes of payload, limited by unsigned byte (255)
  - DRIP uses to carry the FEC

Across  
16-pages



# Forward Error Correction

- Updated to use the Additional Data "field" of F3411-v1.1 Authentication
- With F3411-v1.1, under BT4 we have all 16 pages to work with (minus those needed for actual auth data – itself limited to 9 pages)
- FEC should be page aligned
  - Was page aligned before F3411-v1.1 changes
  - Null bytes added after ADL (to get aligned) and is included in the ADL count
- Need text on Multi-page FEC – Reed Solomon?
- Previous discussion privately on doing FEC for more-than-auth
  - FEC across all messages being sent, not just the Authentication Message
  - This needs to be added soon if we want to include it

# Broadcast Attestation Structure (BAS)

- Generalized format to be used in DRIP Auth. (except Link)
- Change: Removed signing timestamp
  - Pros: more space for attestation data
  - Cons: not in direct alignment with drip-registries Attestation formats

Whenever this structure is used the UA is self-attesting its DET – very important as it confirms possession of key asserted by Broadcast Attestation – more on this later.

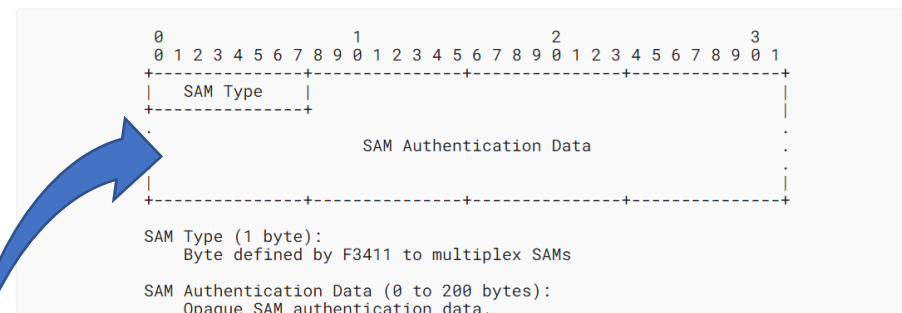


Figure 6: SAM Data Format

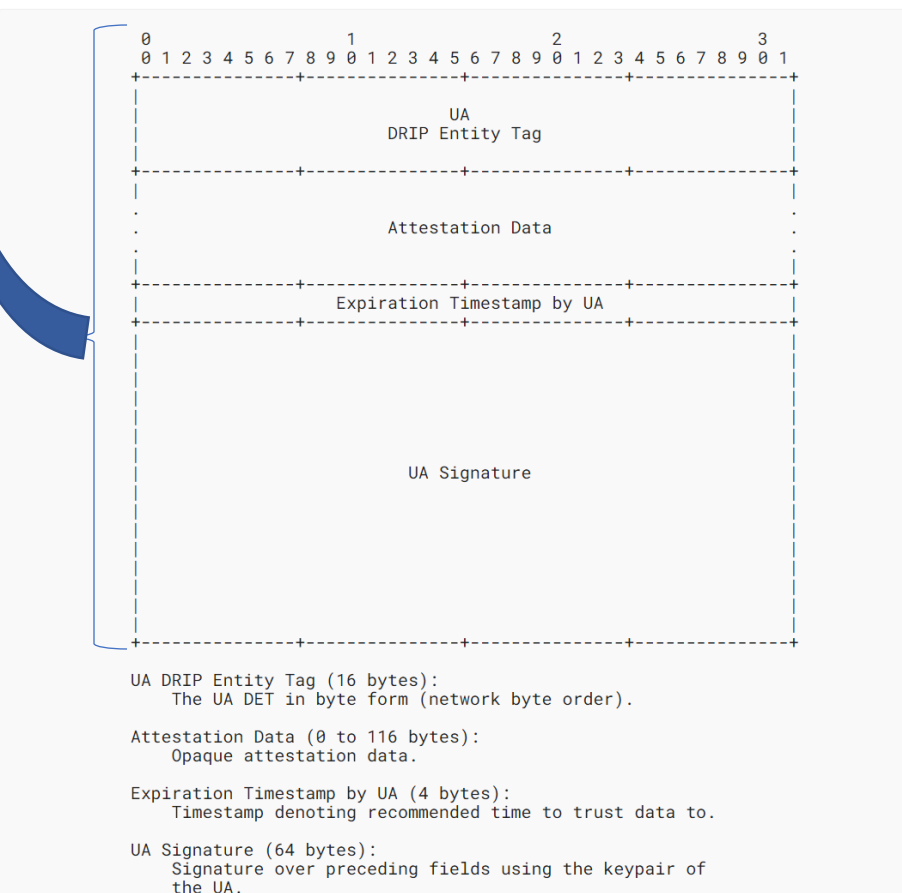


Figure 3: Broadcast Attestation Structure

# DRIP Link

- HDA on UA Broadcast Attestation
- Other Broadcast Attestations can be produced from registry process – do we send them?
- Added Link Type to multiplex
  - Already spilling into a new page, so no waste of adding single byte
  - Future proofing
- Example in Appendix B

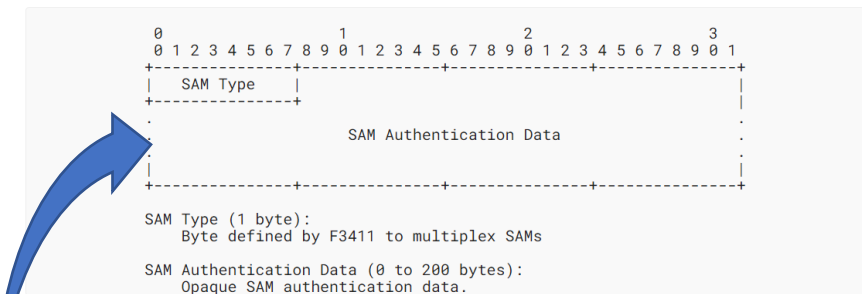


Figure 6: SAM Data Format

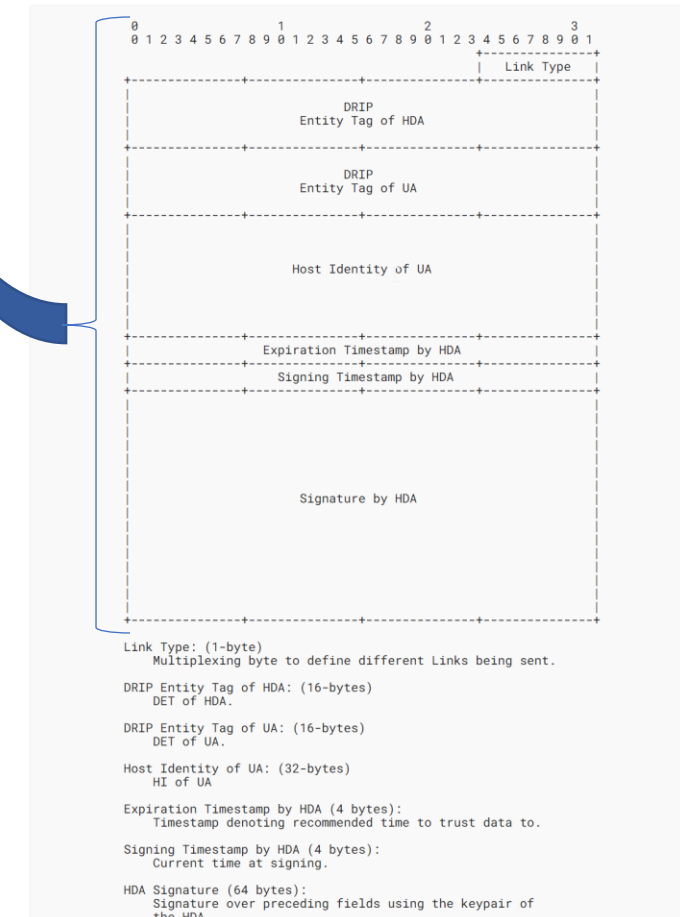


Figure 7: Example DRIP HDA-UA Broadcast Attestation

# DRIP Manifest

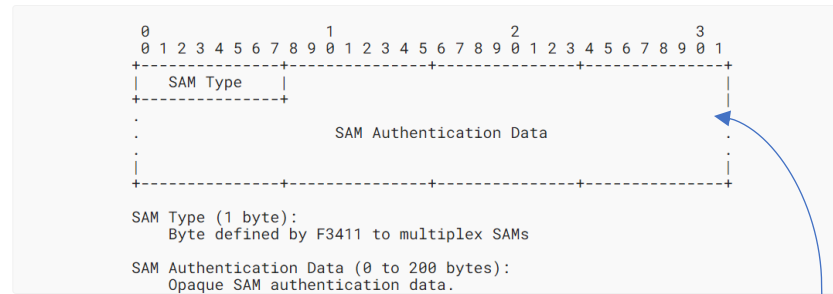


Figure 6: SAM Data Format

- Hash length: 8 to 12
  - Number of hashes lowered to 9 total (7 message hashes)
- Added text to define how to hash messages
  - When Auth. Message, concatenate all pages together into one blob
- Variable Window
  - Needs more text

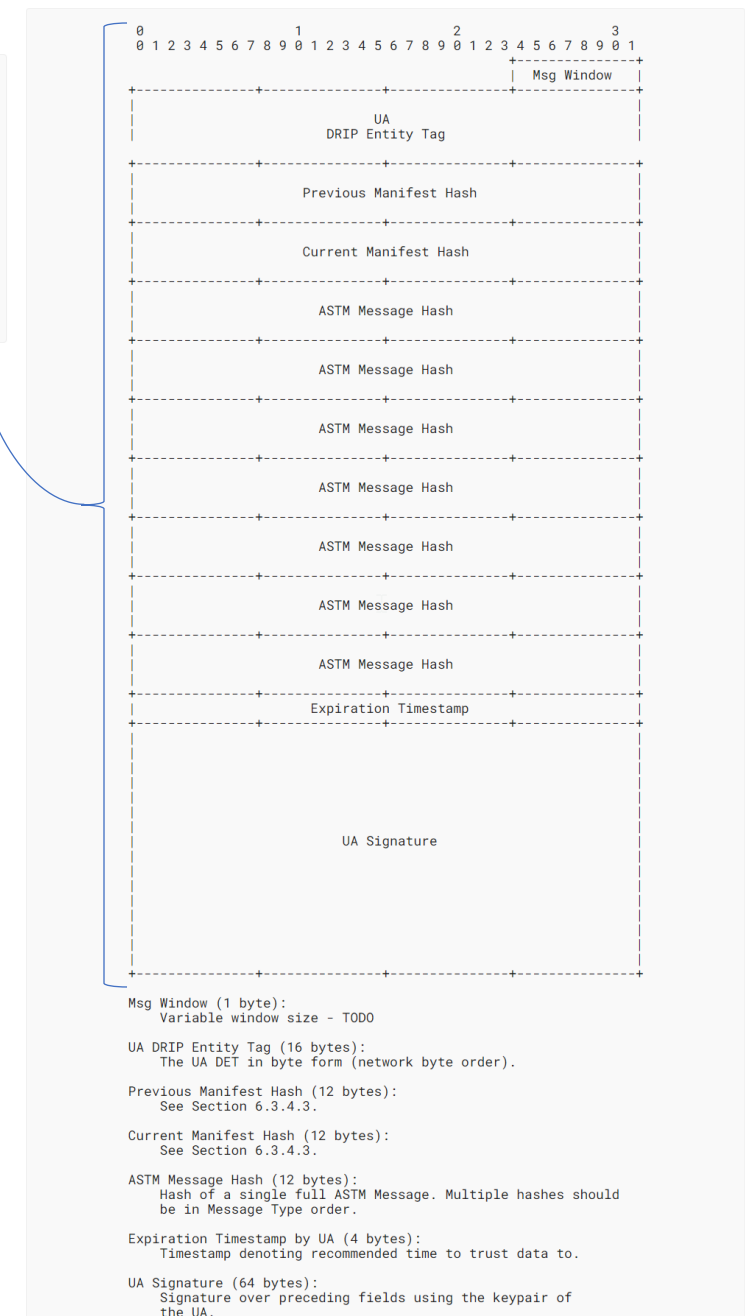
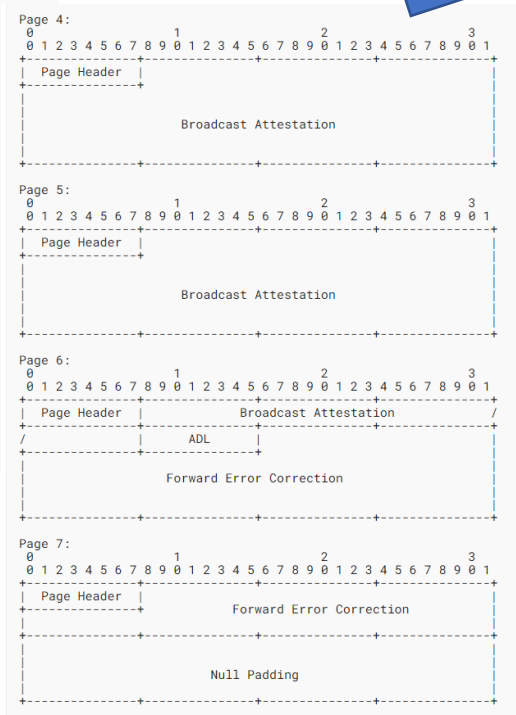
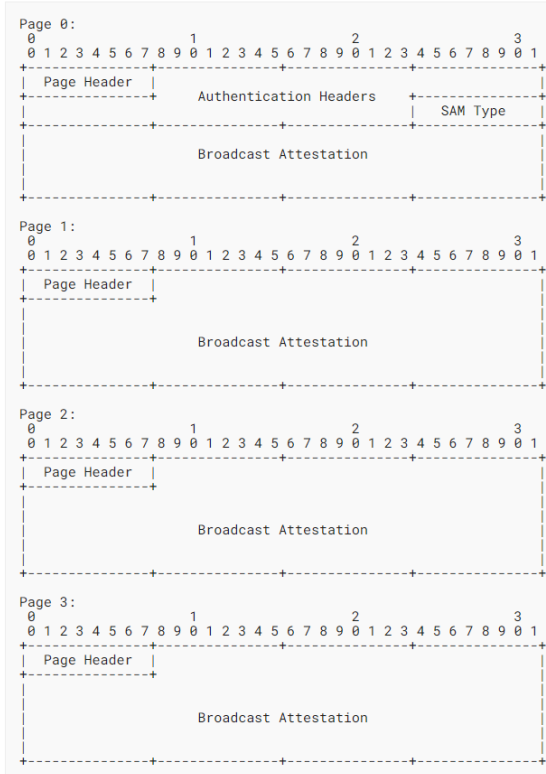


Figure 9: Example DRIP Manifest



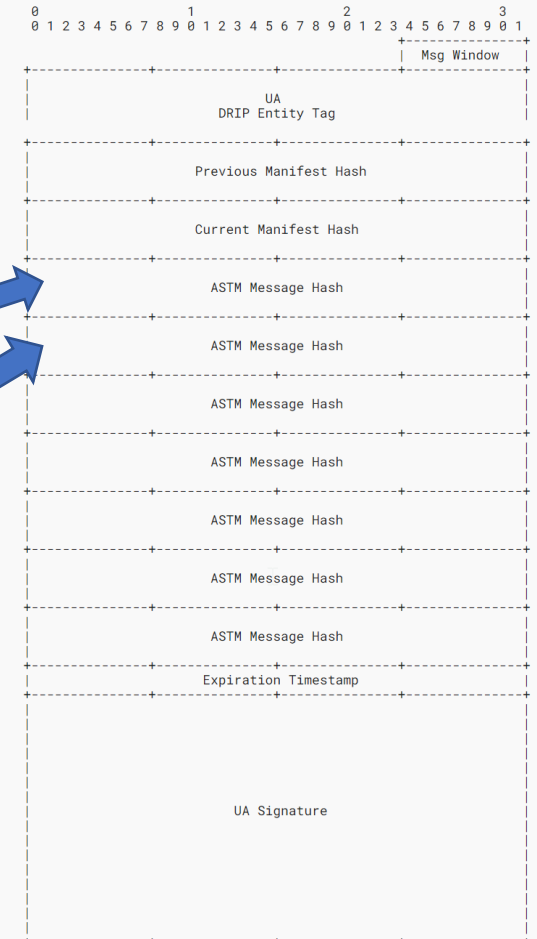
# DRIP Link + Manifest => Trust!

Transmit DRIP Link (left) and hash combined pages of DRIP Link placing into DRIP Manifest (right)...



Hash a Location Message and place into DRIP Manifest....

Sign and send DRIP Manifest – thus validating key ownership assertion!



Msg Window (1 byte):  
 Variable window size - TODO

UA DRIP Entity Tag (16 bytes):  
 The UA DET in byte form (network byte order).

Previous Manifest Hash (12 bytes):  
 See Section 6.3.4.3.

Current Manifest Hash (12 bytes):  
 See Section 6.3.4.3.

ASTM Message Hash (12 bytes):  
 Hash of a single full ASTM Message. Multiple hashes should be in Message Type order.

Expiration Timestamp by UA (4 bytes):  
 Timestamp denoting recommended time to trust data to.

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

Figure 9: Example DRIP Manifest

# DRIP Frame

- More explicit formatting using BAS
- Added byte for multiplexing
  - Future proofing
- Perhaps rename
  - DRIP [UA] Attestation?

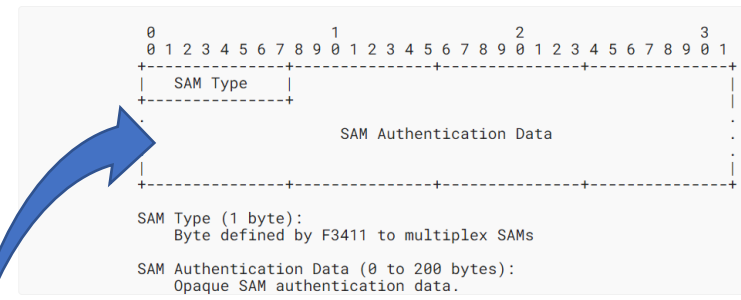
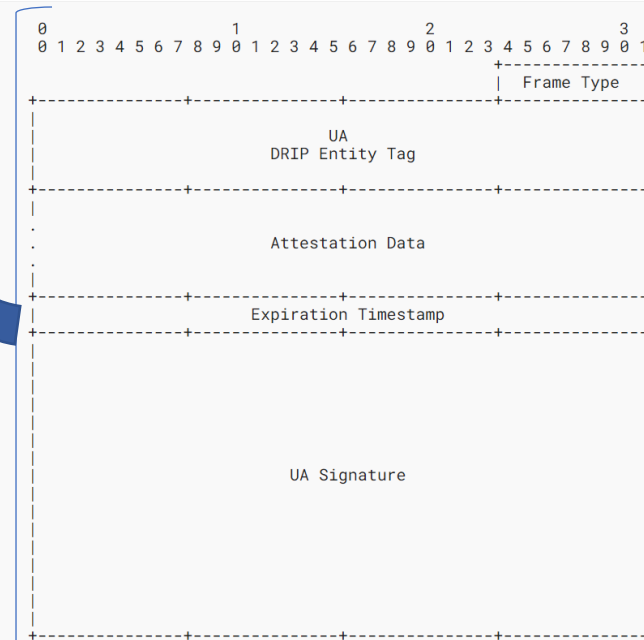


Figure 6: SAM Data Format



Frame Type (1 byte):  
Multiplexing frame type.

UA DRIP Entity Tag (16 bytes):  
The UA DET in byte form (network byte order).

Attestation Data (0 to 115 bytes):  
Opaque attestation data.

Expiration Timestamp by UA (4 bytes):  
Timestamp denoting recommended time to trust data to.

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

Figure 10: Example DRIP Frame

# DRIP Auth. Recommendations / Requirements

- MUST send Link with HDA on UA Broadcast Attestation
- MUST send Manifest with hash of Link & dynamic data (like Location Message)

This is what gives us value: Link asserts a given key is owned by UA and is part of its registry (HDA) + Manifest confirms the key ownership assertion in Link

- Recommends sending other Link messages for other entities
  - Root/RAA, RAA/HDA [, HDA/Operator, Operator/UA]

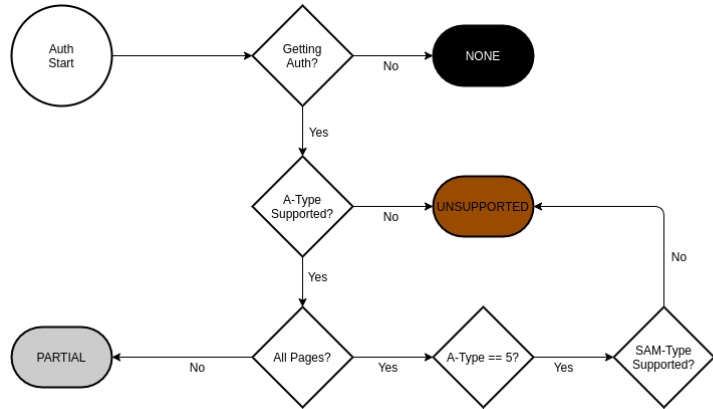
# Operational Recommendations

- Text on how to manage transmission of DRIP messages
  - Up to implementation but best practice given
  - Link every 3s, Manifest directly after a "set" of messages
    - Set is Basic ID, Location, DRIP Link Auth., System [, Operator ID in EU]
  - Overall hard to quantify but good that its mentioned – brings awareness to implementor
- Wrapper special case
  - For map displays to easily mark trusted "dots" in a track
  - Points out that optimization of sending data only in Wrapper cannot be done – makes messages "non-existent" to non-DRIP aware receivers

# Appendices

- Old Appendix A replaced with place-holder for Authentication Coloring Schemes
  - State diagram for recommended receiver authentication states and coloring
- Appendix on Attestations moved to drip-registries
- Appendices moved into main document
  - Forward Error Correction (now Section 4)
  - Broadcast Attestation Structure (now Section 5)
- New Appendix for examples

# Authentication State/Coloring



## Color Priority

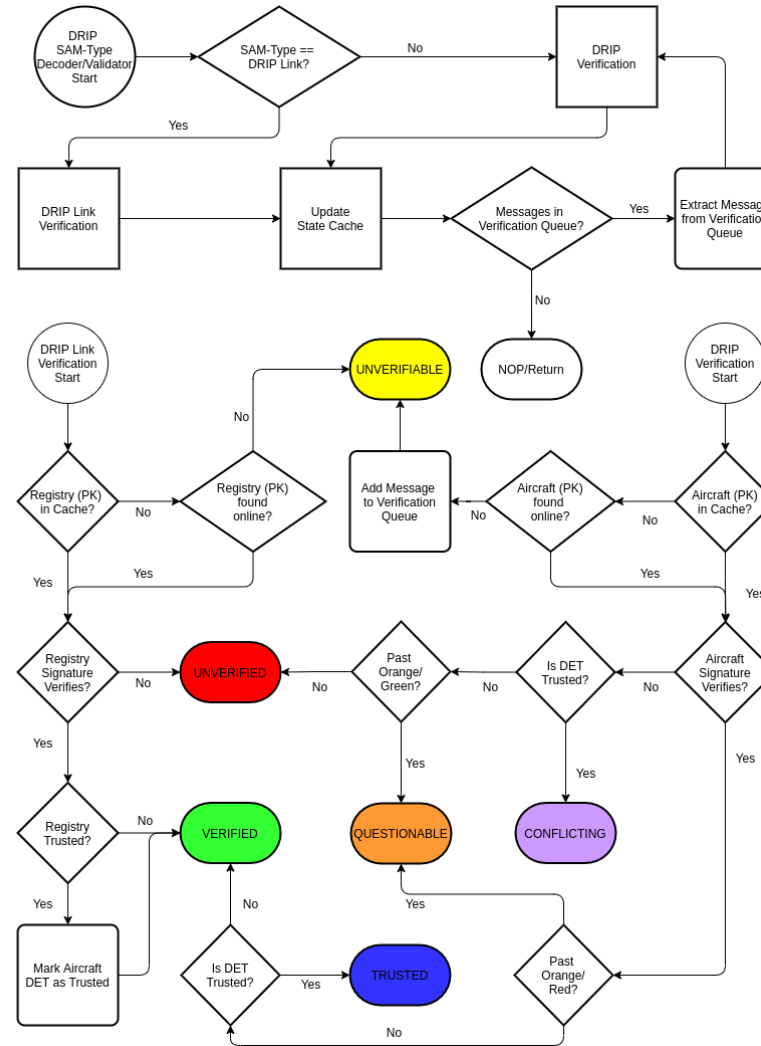
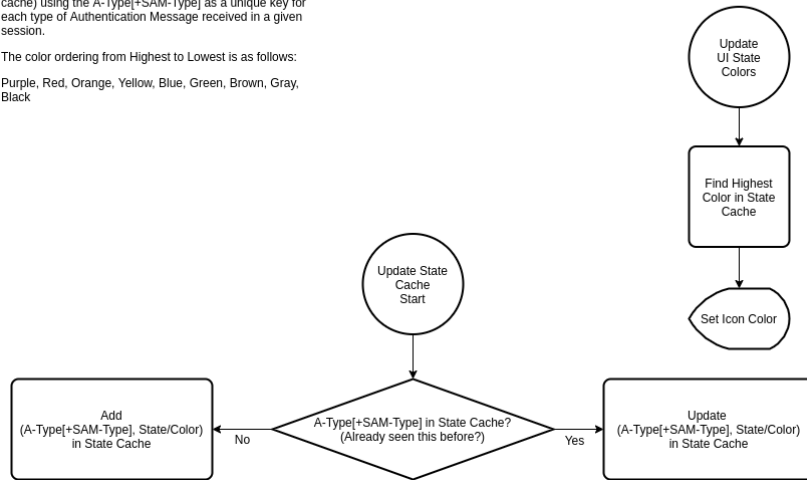
Selection of color at the UI is determined by looking at the various unique Auth Messages received and selecting the Highest color detected for a given UAS ID.

A UAS ID in this context is the combination of the detected MAC Address and declared UAS ID.

Authentication Messages are stored in a cache (state cache) using the A-Type+SAM-Type as a unique key for each type of Authentication Message received in a given session.

The color ordering from Highest to Lowest is as follows:

Purple, Red, Orange, Yellow, Blue, Green, Brown, Gray, Black



# TODOs

- Bob M. pointed out signing of short (<56-byte) messages
  - He will review this, may need to add "context" to signing data to pad
- FEC – Multi-page Reed Solomon, page alignment? more-than-auth?
- Better text on Manifest Variable Window
- Operational Recommendations
  - Bob M. provided bulk of text, will need to be reviewed and iterated over at least once
- IANA Considerations – for new multiplexing bytes of Frame/Link
- Appendix A – need diagram and explanation text
- Appendix B – add hex examples
- Flow diagram – suggestion from Med.
- WGLC?

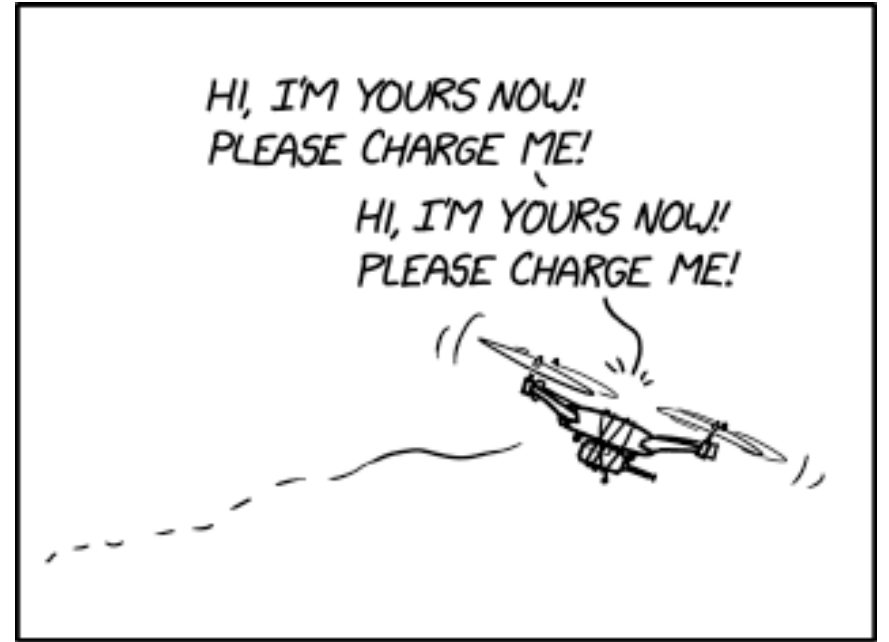
# Next Steps

- Release a new version (-04) that fixes the pending issues listed in last slide (Mid December 21)
- Request early IOTDIR and SECDIR reviews based in that version (give 4 weeks to get the reviews)
- Release a new version that addresses the various reviews (Jan-Feb 22)
- Based on how these items are progressing, we will decide if we will issue the WGLC before or after IETF#113.



# Discussion

Questions, Comments, Concerns?



TECH TIP: IF YOU EVER GET TIRED OF A TOY DRONE, TIE THE CONTROLLER TO IT AND SET IT OUTSIDE. ITS ABANDONMENT FUNCTION WILL ACTIVATE AND IT WILL FIND A NEW HOME.

Remember to only adopt domesticated drones that specifically request it. It's illegal to collect wild ones under the Migratory Drone Treaty Act.

<https://xkcd.com/2499/>