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
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

Figure 1: Standard ASTM Authentication Message Page
Figure 2: ASTM Authentication Message Format
Figure 6: SAM Data Format

DRIP WG -- IETF 112 -- Nov. 11, 2021
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.
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
DRIP Manifest

- 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
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!
DRIP Frame

• More explicit formatting using BAS
• Added byte for multiplexing
  • Future proofing
• Perhaps rename
  • DRIP [UA] Attestation?
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 it's 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-existant" 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 state is determined by looking at the various unique A/MAC messages received and selecting the highest color selected for a given A/MAC.
A MAC/Color combination is the combination of the detected A/MAC address and declared (A/MAC).
Authentication Messages are stored in a cache (state cache) using the A/MAC=ASAM Type as a unique key for each type of Authenticatable Message revealed to a given A/MAC.
The color ordering from highest to lowest is as follows:
Purple, Red, Orange, Yellow, Blue, Green, Brown, Gray, Black

Update UI State Colors (Priority in set UI)
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.
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/