DRIP Authentication Formats

draft-wiethuechter-drip-auth-00

Adam Wiethuechter

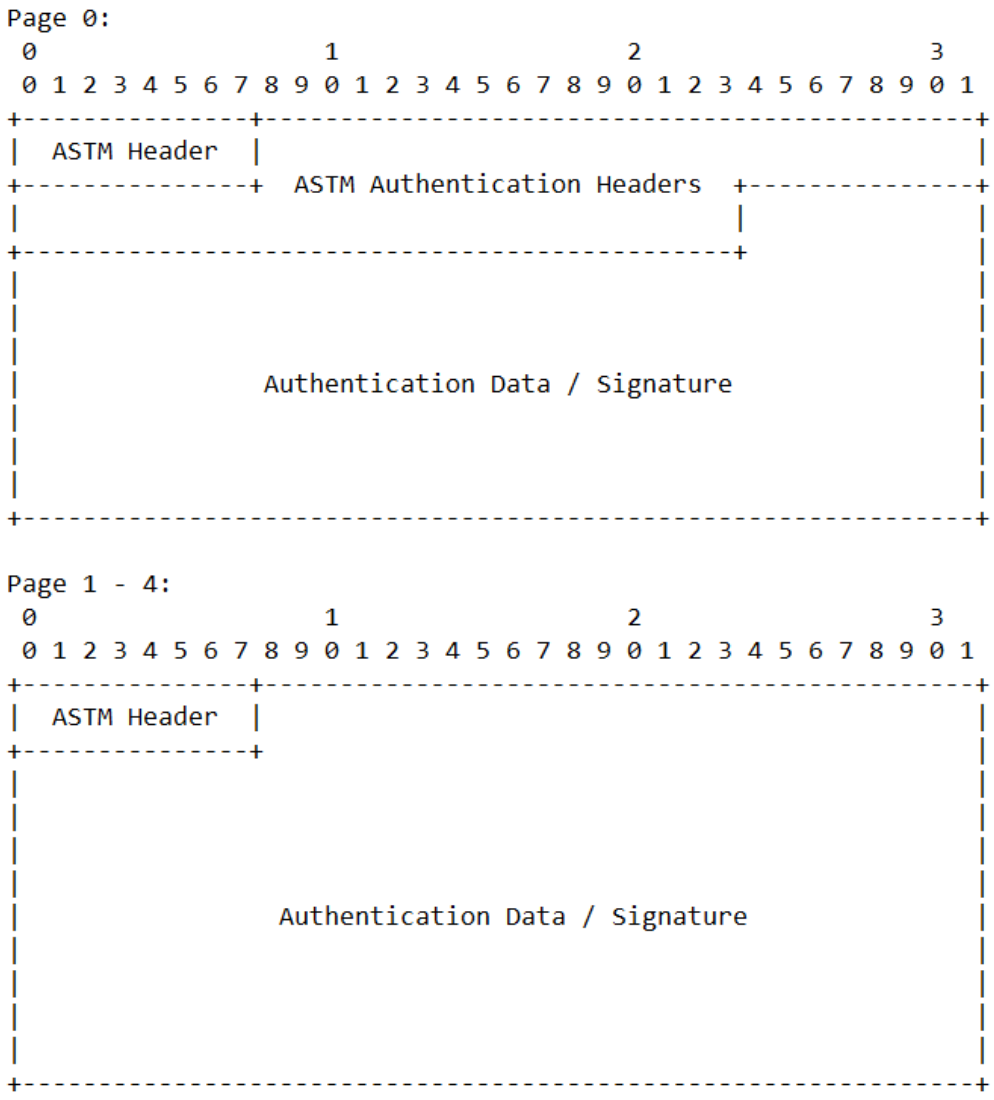
DRIP WG – IETF 107; March 25, 2020

Background

ASTM Authentication Format & Bluetooth 4.X Format

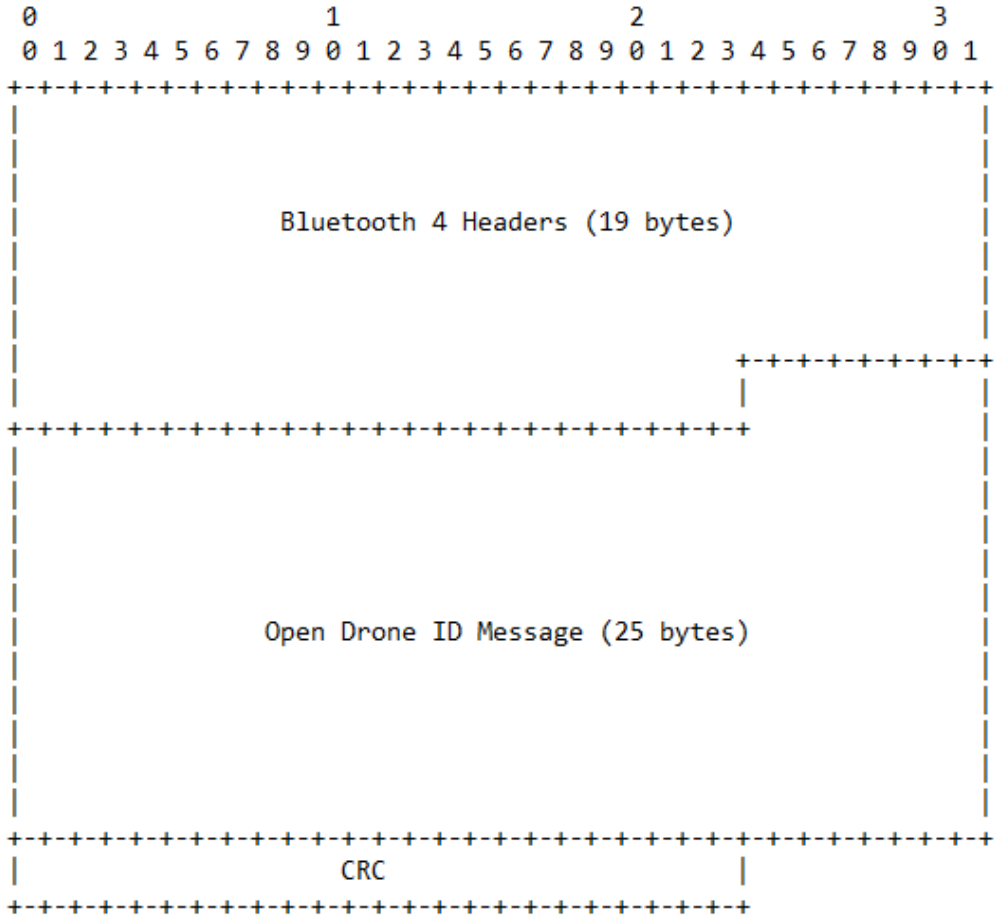
ASTM Authentication

- ASTM F3411-19 “Standard Specification for Remote ID and Tracking”
- Authentication message
  - 5 pages long with a 109 byte max payload (17 + 23 * 4)
  - Designed to authenticate Message Packs (of up to 5 messages in Bluetooth 5.X frame)



Bluetooth Background

- Why so small?
  - Bluetooth 4 legacy frames only give 25 bytes to play with (after Bluetooth headers)
  - 1 byte is for a main header in ASTM format that is always present – now only 24 bytes of data to work with
  - Auth. message has its own header + other fields

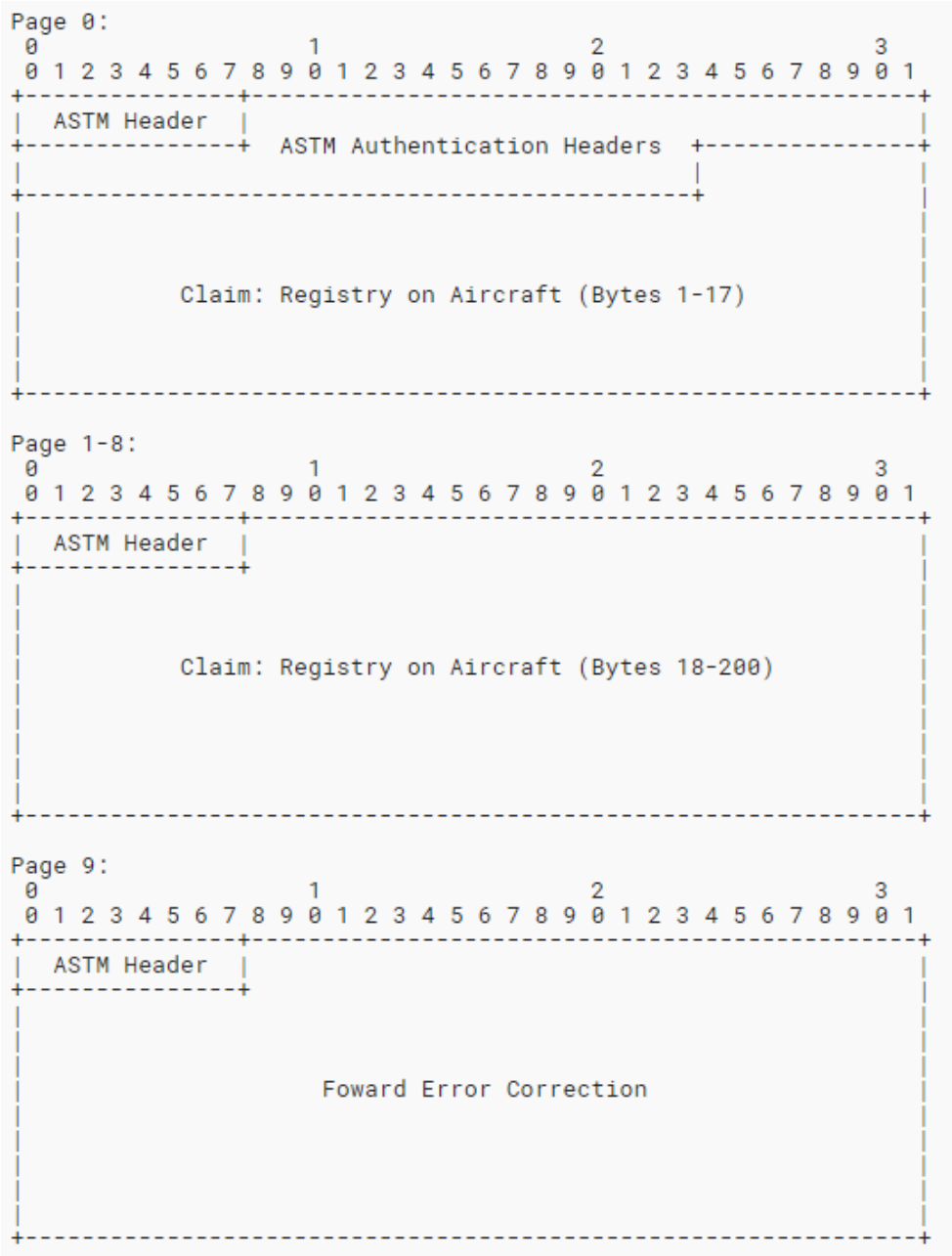


DRIP Message Formats

Claim, Message Wrapper [w/FEC], Signed Hash Lists

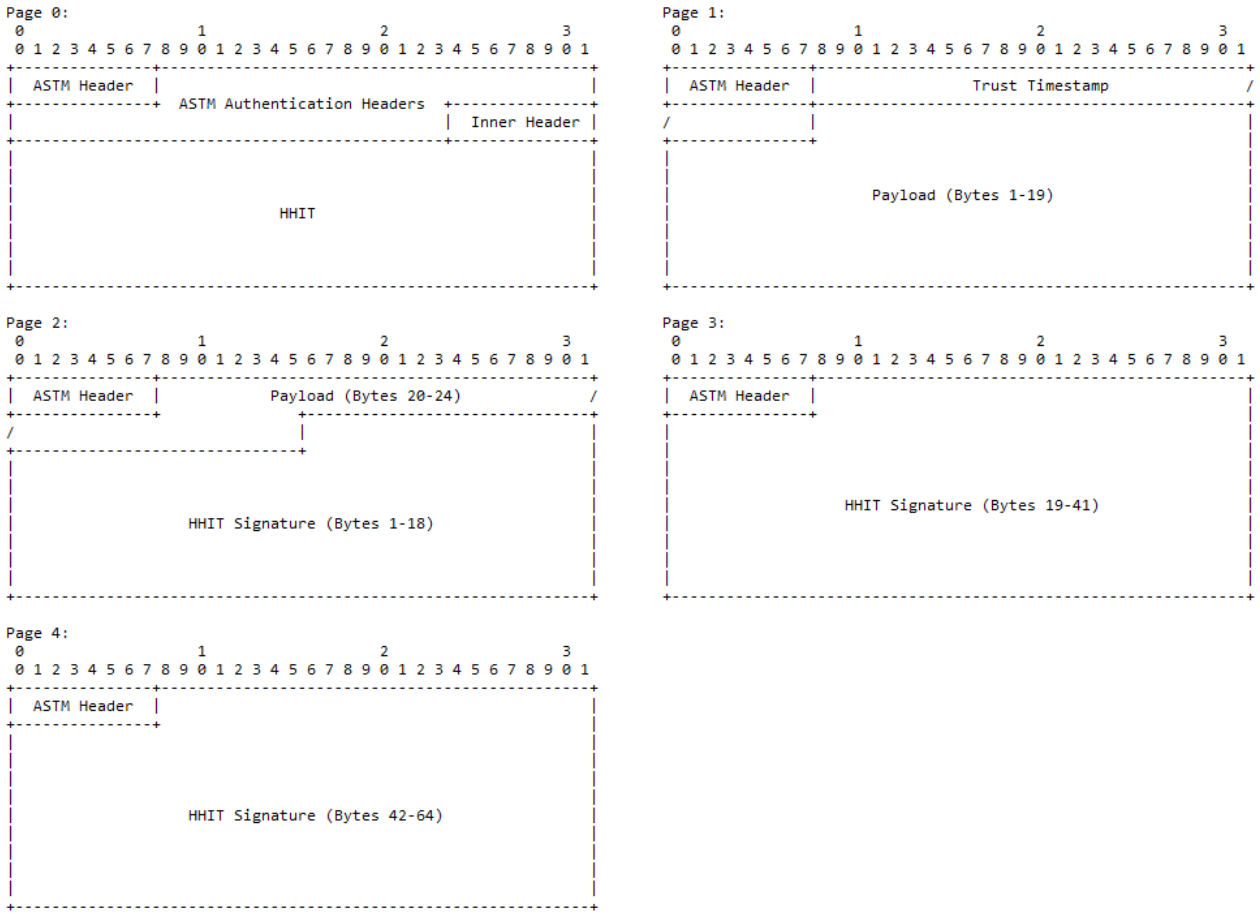
Claim

- Broadcast of “Claim: Registry on Aircraft”
  - Binding between entities, asserting trust
- Contains HI of UA; instant verification of UA
- Registry HHIT used for lookup on local cached Registry list
  - On Observer device, only ones trusted by User
- Need ASTM to update to allow 10 pages
- What form of FEC?
  - Current draft specifies Reed Solomon



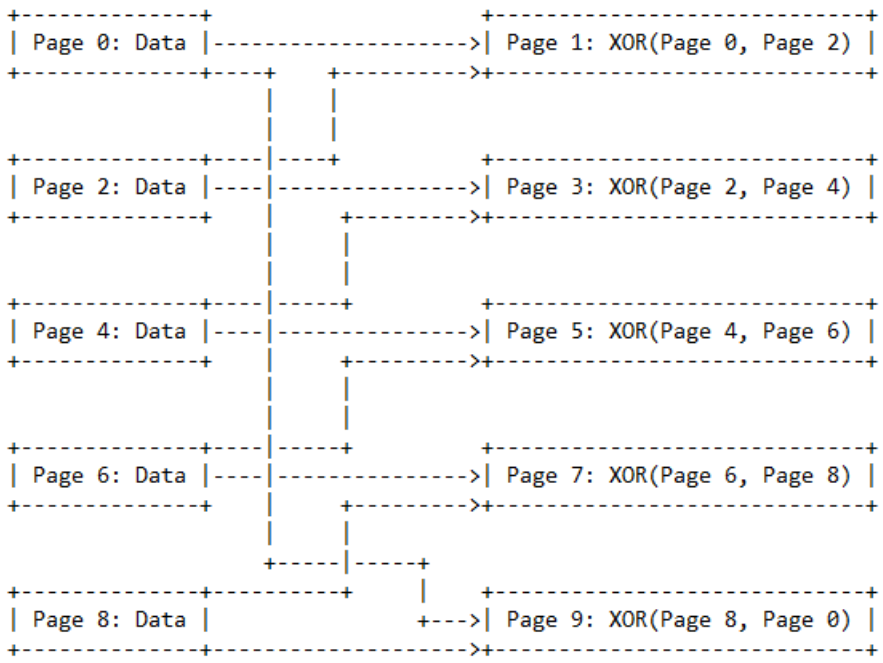
Message Wrapper

- Designed to wrap existing ASTM messages and/or provide framing to create trust using HHITs
- HI lookup from DNS (using HHIT) or from received Claim
- Updates
  - Moved Payload before Signature
  - Added Inner Header



Message Wrapper w/Forward Error Correction (NEW)

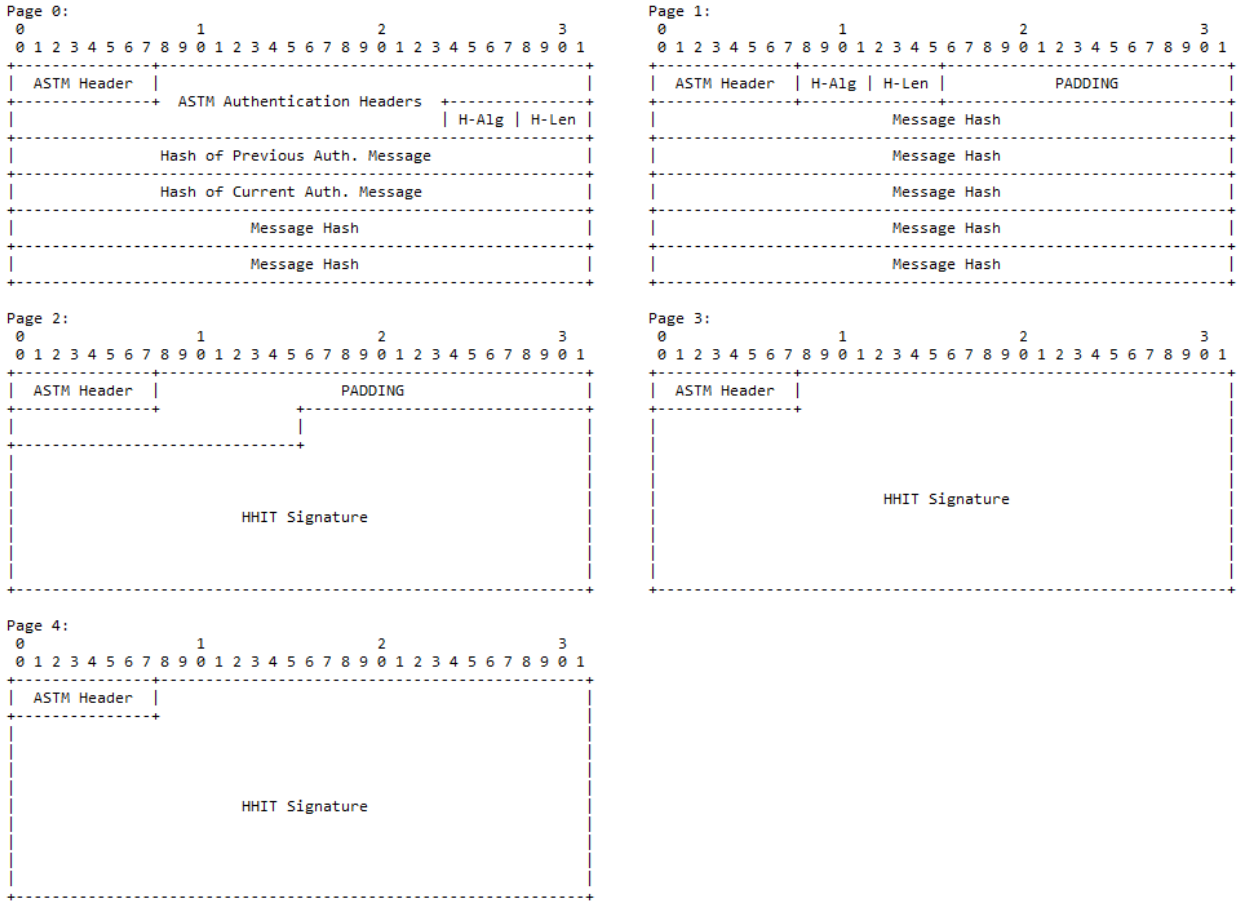
- Reed Solomon
  - Adds one extra page to Message Wrapper format (5 -> 6)
  - Create 23-bytes of parity across whole format
  - Can recover from any single page loss
- Experimental XOR
  - Requires 10 pages
  - Linking XORs across pages (see diagram to right)
  - Can recover (in principle) from numerous pages lost
  - Most likely unhelpful unless in extreme cases

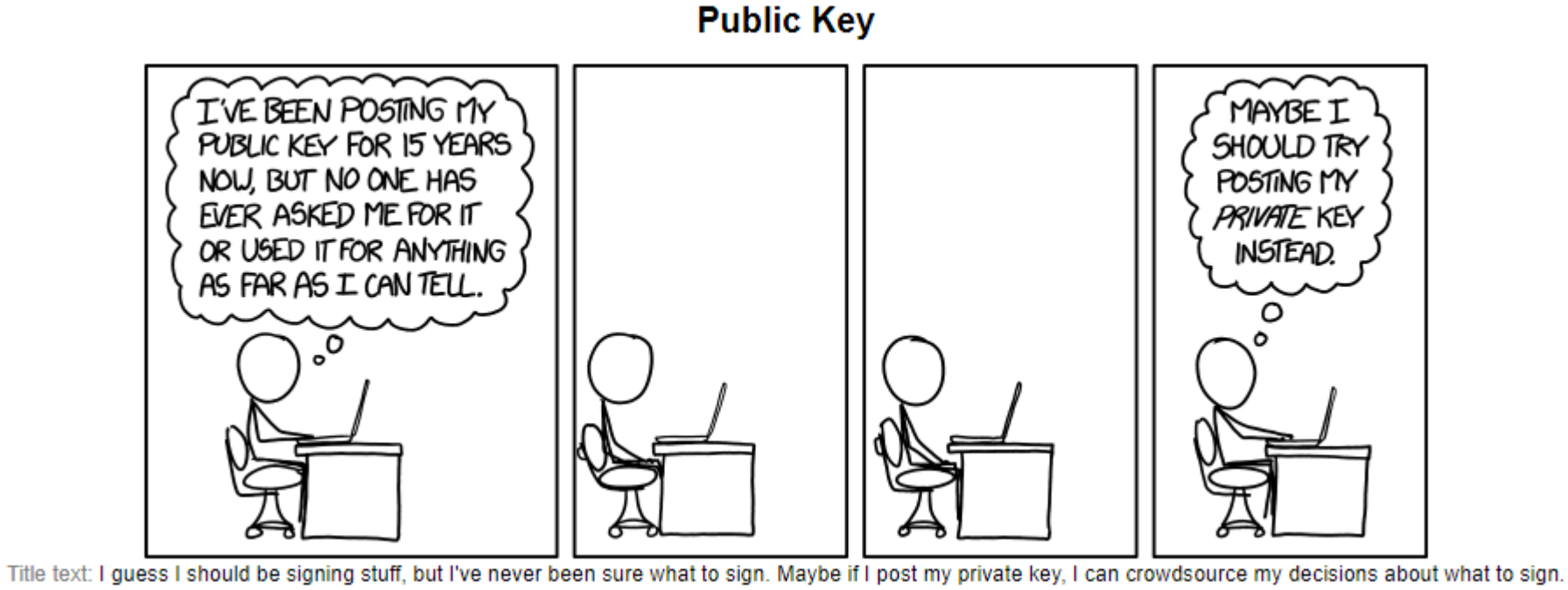


Relationship of pages in Experimental XOR

Signed Hash List

- Provides provenance to previously sent messages
  - Agility through H-Alg and H-Len fields
  - Pseudo-blockchain hashes to link signed lists together
- Could also use idea in wrapper format
  - Removes pseudo-blockchain hashes, lowers count
- Is the number of hashes worth it?





https://xkcd.com/1553/

Discussion

Questions, Comments, Concerns?