rfc447bis

STIR Interim

5/27/2016

Jon

Changes since -08

- Fixes suggested by Alan Ford on the list
- Verification service failure handling for multiple Identity headers
- Cleaned up status codes (see 13.3)
- Algorithm fix (ES256)
  - Also deprecated the “alg” registry
- Outsourcing more to PASSporT (e.g. “mky”)
- Also, added some more Date fix text
- Removed gatewaying section

- Last couple months been a bit quiet… because everyone is happy, right?

When to “canon”?

- “canon” when an extension requires it
- “canon” when a request has been rejected with a 428

- How big a deal is ~100 bytes of redundancy?
  - Though, with “mky” and extensions, it could be considerably more
- Also, is it a privacy risk?

Date Fix (redux)

- So, some intermediaries munge the Date header in the field
  - You are bad and you should feel bad
- The fix here is to allow auth services to resend requests with “canon” when verification fails (438)
  - “canon” contains the base64 encoded JWS header/claims component of PASSporT
  - Date can be constructed from “iat” and used by the verifier to maintain integrity
  - Also, “canon” in general useful for debugging

Status Codes

- Most fixes required for multiple Identity headers
  - General principle: only mandate an error response if there are no acceptable Identity headers
    - At least one viable? Then it's not an error
  - Also requires changes for "ppt"
- 428 (sent if no Identity with supported "ppt")
- 436 now "Bad Identity info"
- 437 now "Unsupported Credential"
- 438 now encourages resending with "canon"

Still To Do

- Backwards compatibility text
- Final(?) editorial pass and clean-up
  - Lot of surgery, been trying to remove scars
  - Like the alg registry, and the gatewaying section
- Do we care about alternative credential systems?
  - If so, we could beef up the requirements on them a bit
- I think this is pretty close