HTTP SCRAM

draft-ietf-httpath-scram-auth-06.txt

Changes since -04

- All SCRAM challenges and responses are now base64-encoded, so existing SASL SCRAM libraries can be used as is.
    - HTTP specific things are added as WWW-Authenticate/Authorization directives.
- Some fixes/clarifications to the reauthentication mode.
- Switched to recommending SHA-256 as Mandatory-to-Implement.
- Clarified that Authentication-Info can be in HTTP trailer.
- Minor ABNF cleanup.

Open Issues/To Do

- Username/password canonicalization before hashing
    - Use StringPrepBis (Precis WG) - draft-ietf-precis-saslprepbis-18 is in RFC Editor's queue
- Do we need "stale" directive like in Digest?

Open Issues

- Maintaining session state (as SCRAM requires 2 round trips)
  - Use "sid" directive?
  - Use a separate header field (e.g. Microsoft's proposal: draft-montenegro-httpbis-multilegged-auth-01)?

Next steps

- Proof read text to make sure it is not very SASL specific and clear
- Implement reauthentication mode
    - Help would be appreciated!
- Need updated examples with proper hashes