SIP Digest

Rifaat Shekh-Yusef

IETF100, SIPCore WG, Singapore

November 13, 2017

RFC7616 – HTTP Digest

- **Algorithms**:
  - **SHA2-256** as the **default** algorithm.
  - **SHA2-512/256** as a **backup** algorithm.
  - **MD5** for backward compatibility.
- **Quality of Protection**
  - The **qop** parameter is required.
- **IANA Registry**
  - Hash Algorithms for HTTP Digest Authentication.

SIP Digest draft

- Updates the **SIP** recommendations to **align** with the **HTTP** recommendations.
  - Uses the same algorithms and their priorities.
  - Updates the SIP ABNF

- https://datatracker.ietf.org/doc/draft-yusef-sipcore-digest-scheme/

SIP Forking

- "…the **forking proxy** server is responsible for **aggregating** these challenges into a **single response**."
- The client is then expected to provide response to one or more of these challenges.

What’s Next?

- Open Issues?
- WG Adoption?