Simple Authentication and Security Layer (SASL) WG

Chairs: Tom Yu, Kurt Zeilenga

IETF 66

Monday, July 10, 2006

15:20–17:20

Agenda

- Intro, scribe, agenda bashing – 5 min

- Document status – 5 min

- DIGEST-MD5 (rfc2831bis) – 40 min

- CRAM-MD5 – 10 min

- GSSAPI / GS2 – 20 min

- Discuss milestones – 10 min

- Open mike – remaining time

Document Status

- `draft-ietf-sasl-crammd5-07.txt`

- `draft-ietf-sasl-gs2-01.txt`

- `draft-ietf-sasl-gssapi-06.txt`

- `draft-ietf-sasl-plain-09.txt`

- `draft-ietf-sasl-rfc2831bis-08.txt`

DIGEST-MD5 (rfc2831bis)

- AES cipher IV

- SASLprep vs other prep

- cnonce same on fast re-auth

- SHOULD vs MUST verify authzid

- RC4 vs AES as mandatory to implement

CRAM-MD5

GS2

Milestones

DONE   SASL (+ EXTERNAL) to IESG

May 06   CRAM-MD5 to IESG

Jul 06   DIGEST-MD5 to IESG

DONE   GSSAPI mech to IESG

Oct 06   Implementation report plan (with milestones)

Nov 06   Revise charter or conclude

Open Mike