Common Authentication Technology Next Generation (kitten)
London, England – IETF 89

Sam Hartman (hartmans-ietf@mit.edu)
Shawn Emery (shawn.emery@oracle.com)
Josh Howlett (josh.howlett@ja.net)

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public."

Overview

- Preliminaries (5 min)
  - Introduction
  - Blue Sheets
  - Scribe, Jabber
  - Remote Participation
  - Agenda Comments
- Active WG Items (15 min)
- GS2 Updates (15 min)
- Update to OAuth Draft (15 min)
- AES-SHA2 (15 min)
- RFC 6112 and 4402 Issues (5 min)
- Per-user Host-based Services and S4U2Proxy Improvements (10 min)
- RFC 5653 Update (5 min)
- Open mic (5 min)

Active WG Items

- IANA-reg (draft-ietf-kitten-gssapi-extensions-iana)
- KRB-IANA-reg (draft-ietf-kitten-kerberos-iana-registries)
- SASL-SAML-EC (draft-ietf-kitten-sasl-saml-ec)
- PKINIT Hash Agility (draft-ietf-krb-wg-pkinit-alg-agility)
- IAKERB (draft-ietf-kitten-iakerb)
- CAMMAC (draft-ietf-krb-wg-cammac)

draft-ietf-kitten-gssapi-extensions-iana

- Provide an initial registry subset in the appendix
- Josh and Alexey have volunteered to work on the initial registry
- Any update?

draft-ietf-kitten-kerberos-iana-registries

- Requesting volunteers to verify assignments to
  - Look at drafts, RFCs, and implementation
  - Verify if any registry entries are missing and if there are any conflicts
  - Where are the registry entries?

draft-ietf-kitten-sasl-saml-ec

- 10 and 11 had been submitted
  - 10: Updated to reference to the final SAML ECP document
  - 11: Normative reference made to RFC 7056
- Scott believes that it is ready for WGLC

draft-ietf-krb-wg-pkinit-alg-agility

- A few updates needed
  - RFC 3766 and RFC 6194 should be informative
  - Error code 82 conflict should be reassigned
    - Deployed code but impact unlikely
- Volunteers to submit new version of the draft?

draft-ietf-kitten-iakerb

- 01 submitted
  - Includes finished message text pulled from PKU2U
  - IANA registry include for IAKERB_PROXY
  - Appendix includes guidance for MIT interoperability
- Is the draft ready for WGLC?

draft-ietf-krb-wg-cammac

- 06 submitted
  - Includes motivation section
  - Open issues
    - Change other-verifiers to [3] SEQUENCE (SIZE (1..MAX)) OF Verifier OPTIONAL
    - Enclose in AD-IF-RELEVANT
  - Do/can consensus calls be made here?

SASL-GS2 Update (15 min)

- Consensus was to remove RFC 5801 requirement for mechanisms to have mutual authentication
  - Simon has volunteered to update the RFC to bis
  - Need volunteers to review update

Updates to OAuth (15 min)

- 12 submitted
  - Removed channel binding section and related text
  - -PLUS related text removed
- Ryan had requested user= to be reintroduced

draft-ietf-kitten-aes-cts-hmac-sha2 (15 min)

- Strong consensus for
  - CTS mode
  - RFC 3961/3962 confounder
- After updates, should be ready for WGLC

RFC 6112 Issues (5 min)

- Sam has submitted draft-ietf-kitten-rfc6112bis
  - Addresses KeyExchange vs. KEYEXCHANGE
  - If an anonymous ticket is used for the PA-TGS-REQ then the anonymous KDC option SHOULD be set in the request

RFC 4402 Issue

- Known implementations have started the PRF counter at 0, not 1
  - Is this universal?
  - Do implementations stop a n or n – 1?
- Should this be an errata or update?
  - Technical → update
- Volunteers to update?

Per-user Host-based Services and S4U2Proxy Improvements (10 min)

- Viktor Dukhovni: slides

RFC 5653 Update (5 min)

- Shawn channeling Max: slides

Open mic (5 min)

- Any comments/questions?