Common Authentication Technology Next Generation (kitten)
Vancouver, BC, CA – IETF 88

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

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- By participating with the IETF, you agree to follow IETF processes.
- If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you must disclose that fact.
- You understand that meetings might be recorded, broadcast, photographed, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

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-[CTS|CBC]-SHA2 (15 min)
- New Draft Adoption (5 min)
- Open mic (5 min)

Active WG Items

- IANA-reg (draft-ietf-kitten-gssapi-extensions-iana)
- 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)
- RFC 6112 Update
- KRB-reg (draft-ietf-kitten-kerberos-iana-registries)

draft-ietf-kitten-gssapi-extensions-iana

- Alexey has made updates based Ben's and Leif's comments
  - One remaining nit on expert reviewer field
- Provide an initial registry subset in the appendix?

draft-ietf-kitten-sasl-saml-ec

- 10 had been submitted
  - Updated OASIS spec referenced

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

- Consensus was that we pull in the finished message text from the PKU2U draft
- Ben had also made a number review comments
- Changes coming soon?

draft-ietf-krb-wg-cammac

- 06 submitted
- Updates made based on review comments
- Remaining open issues
  - Limit the size of other-verifiers?
  - Enclose in AD-IF-RELEVANT?

RFC 6112 Update

- Love had noticed that the cryptographic input was wrong: should be “KEYEXCHANGE” not “KeyExchange”
- Can we have consensus to bring 6112 to historic and update to 6112.bis, rather than create 6112 errata?

draft-ietf-kitten-kerberos-iana-registries

- Status update?

SASL-GS2 Update (15 min) + Updates to OAuth, ... (15 min)

- Consensus
  - Remove requirement for mechanisms to have mutual authentication
  - Any volunteers to help?
- OAuth Update
  - Last revision removes most of GS2 related text
  - Nico commented that the specification must not advertise CB support for a mechanism that may not support mutual authentication
    - Does this require another consensus call?

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

- After moving away from CBC:
  - Can we reach consensus on a modified CTS mode?
  - Should we consider a counter mode?

New Drafts (5 min)

- Consensus to adopt WG item(s)
  - draft-williams-kitten-generic-naming-attributes
  - Was there enough consensus/interest in?:
    - draft-williams-kitten-krb5-pkcross

Open mic (5 min)

- Any comments/questions?