Common Authentication Technology Next Generation (kitten)
Berlin, Germany – IETF 87

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)
- Updates to Oauth draft, OpenID and SAML RFCs (10 min)
- Channel Bound Flag (10 min)
- AES-CTS to CBC (10 min)
- Kerberos Registry to IANA (10 min)
- New Drafts Proposed (10 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)
- KDC Model (draft-ietf-krb-wg-kdc-model)
- 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

- Leif had reviewed and comments on 07
- Provide an initial registry subset in the appendix
- Josh will continue to solicit updates from Alexey

draft-ietf-kitten-sasl-saml-ec

- 07 - 09 had been submitted
  - 07: Credential delegation added
  - 08: Added delegation header
  - 09: Synced delegation constant to ECP document

draft-ietf-krb-wg-kdc-model

- RFC 6880
  - Thanks Leif!

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
- Changes coming soon?

draft-ietf-krb-wg-cammac

- 05 submitted
  - Updates AD-CAMMAC-BINDING to use octet string instead of limiting this to principal name and time stamp
- Is there sufficient interest?

SASL-GS2 Update (15 min) + Updates to OAuth, ... (10 min)

- Consensus
  - Remove requirement for mechanisms to have mutual authentication
- Next steps?
  - Hannes removes GS2 text from current OAuth draft
  - GS2 specification is updated
    - Simon has volunteered to edit/author
    - Any other volunteers?

draft-ietf-kitten-channel-bound-flag (10 min)

- Changes from draft-williams*
  - Based on consensus – support for empty sec ctx
  - New mechanism attributes
    - GSS_C_MA_CBINDING_CONFIRM
    - GSS_C_MA_CBINDING_MAY_CONFIRM
  - New request flag for GSS_Init_sec_context()
    - GSS_C_CB_CONFIRM_FLAG

draft-ietf-kitten-aes-cts-hmac-sha2 (10 min)

- Proposal to switch mode from CTS to CBC with padding as described in RFC 5652::6.3

draft-ietf-kitten-kerberos-iana-registries (10 min)

- Revision 02
  - Number that will not be registered
    - ASN.1 application tag numbers
    - Transited encoding values
    - Protocol version number (pvno) values
- Ready for WGLC?

New Drafts (10 min)

- Proposed drafts as WG items
  - draft-williams-kitten-generic-naming-attributes
  - draft-williams-kitten-krb5-pkcross
- Has anyone read these?

Open mic (5 min)

- Any comments/questions?