Common Authentication Technology Next Generation (kitten)
Honolulu, Hawaii, USA – IETF 91

Shawn Emery (shawn.emery@oracle.com)
Ben Kaduk (kaduk@MIT.EDU)
Matt Miller (mamille2@cisco.com)

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)
- SASL-OAuth (15 min)
- PKINIT Freshness (20 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-alg (draft-ietf-krb-wg-pkinit-alg-agility)
- IAKERB (draft-ietf-kitten-iakerb)
- GSS-Loop (draft-ietf-kitten-gss-loop)
- Channel Bound (draft-ietf-kitten-channel-bound-flag)
- GS2 Update (draft-josefsson-kitten-gs2bis)
- 6112 Update (draft-ietf-kitten-rfc6112bis)
- 5653 Update (draft-ietf-kitten-rfc5653bis)
- 4402 Update (draft-ietf-kitten-rfc4402bis)

draft-ietf-kitten-gssapi-extensions-iana

- Provide an example registry in the appendix
- Examples posted with feed-back and proposed changes
- Should be ready for WGLC after this update

draft-ietf-kitten-sasl-saml-ec

- Sam has reviewed and made some comments on rev 11
  - Scott has not had time to make an update based on these comments
  - Should be able to make these updates during the holiday

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
- Still looking for volunteers to submit new version of the draft

draft-ietf-kitten-iakerb

- Review comments from Nordgren, Greg, and Ben need to be incorporated into a new rev
- Ben has rev'ed to draft to 02 based on these comments
- Followup comments from Greg and Nico
- New rev required, including changes for a full ASN.1 module

draft-ietf-kitten-gss-loop

- Update made to correct/clarify example code
- WGLC expired on 10/29
  - Number of review comments were made
  - Based on the proposed changes is another WGLC required?

draft-ietf-kitten-channel-bound-flag

- Ben had made some comments on the Design section and including an error out state for GSS_Init_sec_context()
- Looking for volunteers to make updates

draft-josefsson-kitten-gs2bis

- Nico had comments
  - Need feedback from Simon
- Still need more reviewers
  - Volunteers?

draft-ietf-kitten-rfc6112bis

- Anonymity Support for Kerberos
- Updated to fix
  - KeyExchange vs. KEYEXCHANGE issue
  - MUST to SHOULD for setting anonymous option when an anonymous ticket is used
- Ready for WGLC
  - Some typos

draft-ietf-kitten-rfc5653bis

- GSS-API Version 2: Java Bindings Update
- Updated to fix
  - Add new field to GSSException class for error token
- Ready for WGLC
  - Some typos

draft-ietf-kitten-rfc4402bis

- A Pseudo-Random Function (PRF) for the Kerberos V GSS-API Mechanism
- Update fixes
  - Counter starts at 0 to match multiple implementations
  - Test vectors included (provided by Greg)
- Ready for WGLC
  - Some typos

SASL-OAuth (15 min)

- Bill Mills will discuss WGLC comments regarding client ID canonicalization

PKINIT Freshness (20 min)

- Andrei Popov will discuss the proposal outlined in draft-short-pkinit-freshness
- Review comments from the list centered on whether to standardized the freshness token

Open mic (5 min)

- Any comments/questions?