Krb-wg IETF75

Friday, July 31st, 2009
Morning Session 0900-1130

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
  - 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.

How to Participate Remotely

- Jabber: krb-wg@jabber.ietf.org
- Audio: http://feed.verilan.com/ietf/stream04.m3u
- Jabber log: http://jabber.ietf.org/logs/krb-wg/

WG Information

- Web page: charter, current documents

  http://www.ietf.org/dyn/wg/charter/krb-wg-charter.html

- Mailing List: ietf-krb-wg@lists.anl.gov
  To Subscribe: https://lists.anl.gov/mailman/listinfo/ietf-krb-wg
  Archive: https://lists.anl.gov/pipermail/ietf-krb-wg/

- Chairs:
  - Larry Zhu   larry.zhu@microsoft.com
  - Jeffrey Hutzelman   jhutz@cmu.edu
- Security Area Director:
  - Tim Polk   tim.polk@nist.gov

Agenda

- Administrivia - Blue sheets, note takers, etc (5 min)
- Document status (20 min)
- Preauth framework (Sam Hartman and Larry Zhu – 10 min)
  http://www.ietf.org/id/draft-ietf-krb-wg-preauth-framework-12.txt
- Kerberos hash Update(Tom Yu - 10 min)
  Input from Kerberos consortium
- DHCPv6 Kerberos option (Shoichi Sakane - 15 min)
  http://www.ietf.org/id/draft-sakane-dhc-dhcpv6-kdc-option-04.txt
- IA-Kerb Update (Larry Zhu - 5 minutes)
  http://tools.ietf.org/html/draft-ietf-krb-wg-iakerb-01
- Open MIC (10 min)

Document Status

- StartTLS
  - draft-josefsson-kerberos5-starttls-06.txt
  - draft-josefsson-krb5starttls-bootstrap-02.txt
  - Ready to be published as is
  - Informational
  - No open issue (?)
  - Waiting for chair write-up

Document Status cont'd

- Data model
  - Wait for new revision
- Iakerb
  - Changes made for the one last call comment in -02
  - New changes due to implementation experience
- Ticket extension
  - draft-lha-krb-wg-ticket-extensions-03.txt
  - Work in progress?

Document Status Cont'ed

- DHCP Option
  - draft-sakane-dhc-dhcpv6-kdc-option-04.txt
  - Work in progress
- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-13.txt
  - Basically done
  - Waiting for chair
- Anonymity
  - draft-ietf-krb-wg-anon-10.txt
  - Waiting for chair

Document Status Cont'ed

- Name constraints
  - draft-ietf-krb-wg-naming-07.txt
  - Waiting for chair
- PKINIT Hash agility
  - draft-ietf-krb-wg-pkinit-alg-agility-04.txt
  - Ready for last call
  - Test vectors need to be verified

Document Status Cont'ed

- GSS hash agility
  - draft-ietf-krb-wg-gss-cb-hash-agility-05.txt
  - Waiting for chair
- Cross realm problem
  - draft-ietf-krb-wg-cross-problem-statement-03.txt
  - Need new revision
- Referrals
  - draft-ietf-krb-wg-kerberos-referrals-11.txt
  - Work in progress

Document Status Cont'ed

- OTP
  - draft-ietf-krb-wg-otp-preauth-10.txt
  - New new revision
  - Need another last working group call
  - Tagging issues (closed)
  - Kerberos flags (closed)
  - Password changes (closed)
  - S/Key OTP support (converging)