71st IETF

Kerberos Working Group

Kerberos Working Group Introduction

- Web Page: http://tools.ietf.org/wg/krb-wg/
- Mailing List: ietf-krb-wg@anl.gov
  - Archives: ftp://ftp.ietf.org/ietf-mail-archive/krb-wg/
  - To Subscribe: https://lists.anl.gov/mailman/listinfo/ietf-krb-wg

Kerberos Working Group Meeting Participation

- Audio: http://tinyurl.com/26g8z5
- Jabber: krb-wg@jabber.ietf.org
- Materials: http://tinyurl.com/yv7d3w
- Slides (VNC): ietf-vnc.central.org

Please Use The Mic!

Kerberos Working Group Agenda

- Preliminaries (5 min)
- Document Status (10 min)
- Last Call (30 min)
- Technical Discussion (60 min)
  - Preauth Framework
  - OTP
  - Cross-Realm Directions
- Review and Milestones (10 min)
- Open Mic

Kerberos Working Group Document Status

- Set/Change Password
  - draft-ietf-krb-wg-kerberos-set-passwd-07.txt
  - Needs new revision, then on to IESG
- GSS Agility
  - draft-ietf-krb-wg-gss-cb-hash-agility-03.txt
  - WGLC done; writeup in progress
- Cross-Realm Problems
  - draft-ietf-krb-wg-cross-problem-statement-02.txt
  - Lame chairs will finish review soon

Kerberos Working Group
Last Call

- ECC for PKINIT
  - draft-zhu-pkinit-ecc-04.txt
- Naming
  - draft-ietf-krb-wg-naming-04.txt
- Anonymous
  - draft-ietf-krb-wg-anon-05.txt
- Data Model
  - draft-johansson-kerberos-model-04.txt

Kerberos Working Group
Last Call Issues - Naming

- Security Considerations
  - How can unintented access be granted if authentication is allowed to succeed with an unsupported well-known name?
  - Why is it permissible for the TGS to allow authentication to succeed even if the client and/or server principal name is an unsupported well-known name?

Kerberos Working Group Technical Discussion

- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-06.txt
- One-Time Passwords
  - draft-ietf-krb-wg-otp-preauth-03.txt
- Cross-Realm Directions
  - Client-Friendly Cross-Realm - Kamada Ken’ichi

Kerberos Working Group
Technical Discussion - Preauth Framework

- Recent Changes
- Open Issues

Kerberos Working Group
Technical Discussion - One-Time Password

- Mandatory Mechanism
  - - RFC2289 (OTP)
  - - RFC4226 (OATH)
  - - Do we need one at all?

Kerberos Working Group Milestones

- Aug 2007 — Hash agility for PKINIT to IESG
- Sep 2007 — WGLC on preauth framework
- Nov 2007 — WGLC on OTP
- Nov 2007 — WGLC on hardware preauth
- Dec 2007 — WGLC on data model
- Jan 2008 — WGLC on STARTTLS
- Jan 2008 — WGLC on Referrals
- Mar 2008 — WGLC on Kerberos v5.3
- Mar 2008 — WGLC on IAKERB
- Mar 2008 — WGLC on LDAP schema

Kerberos Working Group

Open Mic