70th IETF

Kerberos Working Group
Kerberos Working Group
Introduction


- Mailing List: ietf-krb-wg@anl.gov
  - To Subscribe: https://lists.anl.gov/mailman/listinfo/ietf-krb-wg
Kerberos Working Group
Meeting Participation

- Audio: http://tinyurl.com/2karj7
- Jabber: krb-wg@jabber.ietf.org
- Materials: http://tinyurl.com/2jwtgj
- 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 (80 min)
  - Preauth Framework
  - Referrals
  - Kerberos v5.3 Directions
- Review and Milestones (10 min)
- Open Mic
Kerberos Working Group
Document Status

- **ECC for PKINIT**
  - draft-zhu-pkinit-ecc-04.txt
  - In AD Review

- **Set/Change Password**
  - draft-ietf-krb-wg-kerberos-set-passwd-07.txt
  - Waiting for PROTO Review Response

- **Data Model**
  - draft-johansson-kerberos-model-04.txt
  - Almost Ready
Kerberos Working Group
Last Call

- **Anonymous**
  - draft-ietf-krb-wg-anon-04.txt
  - WGLC Completed November 21, 2007

- **GSS Hash Agility**
  - draft-ietf-krb-wg-gss-cb-hash-agility-03.txt
  - WGLC Ends Dec 6, 2007

- **Cross Realm Problems**
  - draft-ietf-krb-wg-cross-problem-statement-01.txt
  - WGLC Ends Dec 14, 2007
Kerberos Working Group
Technical Discussion

- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-06.txt

- Referrals
  - draft-ietf-krb-wg-kerberos-referrals-10.txt
Chicago Proposal
- Negotiation via FAST/STARTTLS
- FAST/STARTTLS for Auth Cleartext
- Simplified Protocol Messages
- Ticket Extensions Enctype Hack
- Updates (not Obsoletes) 4120
FAST
- REQUIRED? RECOMMENDED?
- Use for negotiation?

STARTTLS
- REQUIRED? RECOMMENDED?
- Use for negotiation?
- Standards Track?

I18N
Kerberos Working Group
Milestones

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 2007</td>
<td></td>
<td>Hash agility for PKINIT to IESG</td>
</tr>
<tr>
<td>Sep 2007</td>
<td></td>
<td>WGLC on preauth framework</td>
</tr>
<tr>
<td>Nov 2007</td>
<td></td>
<td>WGLC on OTP</td>
</tr>
<tr>
<td>Nov 2007</td>
<td></td>
<td>WGLC on hardware preauth</td>
</tr>
<tr>
<td>Dec 2007</td>
<td></td>
<td>WGLC on data model</td>
</tr>
<tr>
<td>Jan 2008</td>
<td></td>
<td>WGLC on STARTTLS</td>
</tr>
<tr>
<td>Jan 2008</td>
<td></td>
<td>WGLC on Referrals</td>
</tr>
<tr>
<td>Mar 2008</td>
<td></td>
<td>WGLC on Kerberos v5.3</td>
</tr>
<tr>
<td>Mar 2008</td>
<td></td>
<td>WGLC on IAKERB</td>
</tr>
<tr>
<td>Mar 2008</td>
<td></td>
<td>WGLC on LDAP schema</td>
</tr>
</tbody>
</table>
Open Mic