Public Key Infrastructure Using X.509 (PKIX) Working Group

March 28, 2011   1300-1130
IETF 80 - Prague
PKIX WG (pkix-wg)

- Web page: charter, current documents
  - http://datatracker.ietf.org/wg/pkix/charter/
- Mailing List: pkix@ietf.org
  - To Subscribe: pkix-request@ietf.org
  - Archive: http://www.ietf.org/mail-archive/web/pkix/
- Chairs
  - Stephen Kent  kent@bbn.com
  - Stefan Santesson  stefan@aaa-sec.com
- Security Area Director
  - Sean Turner  turners@ieca.com
PKIX Agenda for 80th IETF in Prague

• Introduction
  – Document Status Overview, Stefan Santesson

• WG documents
  – RFC2560bis, Stefan Santesson
  – Issues with RFC2560 and RFC2560bis, Denis Pinkas
  – Enrollment over Secure Transport, Max Pritikin

• Related specifications and Liaison
  – Certificate revocation for high volume websites, Max Pala
  – Security policy flag 'Must be OCSP stapled', Phil Hallam-Baker
  – ClaimSgining EKU, Matt King
  – Authentication context QCStatement, Stefan Santesson
  – OCSP ’Not Issued’ statement, Denis Pinkas
Status since last meeting

• 1 New RFCs published
• 0 documents in RFC Editor’s Queue
• 1 documents in IESG processing
• 6 drafts currently in WG process
New RFCs published

• RFC 6402 – November 2011
  – Certificate Management over CMS (CMC) Updates
In IESG Processing

- AD Evaluation::Revised ID Needed
  - draft-ietf-pkix-cmp-transport-protocols-16
# Active WG Documents

<table>
<thead>
<tr>
<th>Work item</th>
<th>Drafts (draft-ietf-pkix-)</th>
<th>Intended status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarifications to RFC 5280</td>
<td>rfc5280-clarifications-04</td>
<td>Expired (ST)</td>
</tr>
<tr>
<td>OCSP update</td>
<td>rfc2560bis-04</td>
<td>Standards Track</td>
</tr>
<tr>
<td>S/MIME capabilities for pub keys</td>
<td>pubkey-caps-04</td>
<td>Standards Track</td>
</tr>
<tr>
<td>DNS CA authorization resource record</td>
<td>caa-05</td>
<td>Standards Track</td>
</tr>
<tr>
<td>CMC server key generation</td>
<td>cmc-serverkeygeneration-00</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Enrollment over secure transport</td>
<td>est-01</td>
<td>Standards Track</td>
</tr>
</tbody>
</table>