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
  - Tim Polk tim.polk@nist.gov
PKIX Agenda for 80th IETF in Prague

• Introduction
  – Document Status Overview, Stefan Santesson

• WG documents
  – S/MIME Capabilities for Public Key definitions, Jim Schaad
  – OCSP Agility, Stefan Santesson
  – Internationalized e-mail addresses in X.509 certificates, Alexey Melnikov
  – CMC updates, Jim Schaad

• Related specifications and Liaison
  – EU standardization mandate, Steve Kent
  – Future of PKIX enrollment protocols, Joe Salowey
Status since last meeting

• 0 New RFCs published
• 2 documents in RFC Editor’s Queue
• 0 documents in IESG processing
• 5 drafts currently in WG process
• 1 Expired draft
• 1 additional draft under WG review (draft-ietf-hip-cert-09)
In RFC-Editor’s Queue

- Certificate Image
  - draft-ietf-pkix-certimage-11
- OCSP Agility
  - draft-ietf-pkix-ocspagility-10
## 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>CMC Updates</td>
<td>rfc5272-bis-01</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Clarifications to RFC 5280</td>
<td>rfc5280-clarifications-01</td>
<td>Expired (ST)</td>
</tr>
<tr>
<td>OCSP update</td>
<td>rfc2560bis-02</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Transport Protocols for CMP</td>
<td>cmp-transport-protocols-10</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Internet mail addresses in X.509</td>
<td>eai-addresses-00</td>
<td>Standards Track</td>
</tr>
<tr>
<td>S/MIME Capabilities for pub keys</td>
<td>pubkey-caps-01</td>
<td>Standards Track</td>
</tr>
</tbody>
</table>