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

July 29, 2009    1300-1500
IETF 75 - Stockholm
PKIX WG (pkix-wg)

- Web page: charter, current documents

- Mailing List: ietf-pkix@imc.org
  - To Subscribe: ietf-pkix-request@imc.org, In Body: subscribe
  - Archive: http://www.imc.org/ietf-pkix

- Chairs
  - Stephen Kent kent@bbn.com
  - Stefan Santesson stefan@aaa-sec.com

- Security Area Directors
  - Tim Polk tim.polk@nist.gov
  - Pasi Eronen pasi.eronen@nokia.com
PKIX Agenda for 75\textsuperscript{th} IETF in Stockholm

- Introduction
  - Document Status Overview, Stefan Santesson

- WG documents
  - Trust Anchor Management (TAM), Carl Wallace
  - OCSP Algorithm Agility, Stefan Santesson
  - Time-Stamp Protocol update, Stefan Santesson
  - Certificate Image, Stefan Santesson
  - Algs and identifiers for DS and ECDSA, Tim Polk

- Related specifications and Liaison
  - Certificate Information Expression, Stefan Santesson
  - Relying party software tool development for SIDR, Stephen Kent
Status since last meeting

- 0 New RFCs published
- 3 documents in RFC Editor’s Queue
- 3 new documents in IESG
- 9 drafts representing 8 work items currently in WG process
RFC Editor’s Queue

• Update for RSAES-OAEP Algorithm Parameters (rfc4055-update-02) – waiting for 3281bis
  – draft-ietf-pkix-rfc4055-update-02

• Attribute Certificate Profile - 3281bis
  – draft-ietf-pkix-3281update-05

• Traceable Anonymous Certificate
  – draft-ietf-pkix-tac-04
In IESG process

• In IETF Last Call
  – Clearance Attribute and Authority Clearance Constraints
    • draft-ietf-pkix-authorityclearanceconstraints-02
  – Other Certificates Extension
    • draft-ietf-pkix-other-certs-04

• Scheduled for telechat August 13
  – Trust Anchor Format
    • draft-ietf-pkix-ta-format-03
# 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>Additional Algorithms and Identifiers for DSA and ECDSA</td>
<td>sha2-dsa-ecdsa-06</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Trust Anchor Management</td>
<td>ta-mgmt-reqs-03 tamp-02</td>
<td>Standards Track (Informational Requirements)</td>
</tr>
<tr>
<td>New ASN.1 Modules for PKIX</td>
<td>new-asn1-05</td>
<td>Standards track</td>
</tr>
<tr>
<td>PKI Resource Query Protocol (PRQP)</td>
<td>prqp-03</td>
<td>Experimental</td>
</tr>
<tr>
<td>Time Stamp Protocol Update</td>
<td>rfc3161bis-01</td>
<td>Standards Track</td>
</tr>
<tr>
<td>OCSP Algorithm Agility</td>
<td>ocschapagility-00</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Certificate Image</td>
<td>certimage-00</td>
<td>Standards Track</td>
</tr>
<tr>
<td>ASN.1 Translation</td>
<td>asn1-translation-00</td>
<td>Informational</td>
</tr>
</tbody>
</table>