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

November 18, 2008 1520 - 1720
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 stefans@microsoft.com
- Security Area Directors
  - Tim Polk tim.polk@nist.gov
  - Pasi Eronen pasi.eronen@nokia.com
PKIX Agenda for 72\textsuperscript{nd} IETF in Dublin

- **Introduction**
  - Document Status Overview

- **WG documents**
  - Other-certs extension, Stephen Farrel
  - PKI Resource Query Protocol, Massimiliano Pala
  - Attribute Certificate Profile Update - 3281update, Sean Turner
  - ECC Subject Public Key Information, Sean Turner
  - Traceable Anonymous Certificate (TAC), SangHwan Park
  - Clearance and CA Clearance Constraints, Sean Turner
  - Trust Anchor Management (TAM), Carl Wallace

- **Related specifications and Liaison**
  - OCSP Algorithm Agility, Phil Hallam-Baker
  - Time-Stamp Protocol update, Stephen Kent OBO Denis Pinkas
Status since last meeting

• 0 New RFCs published
• 2 documents in IESG
• 11 drafts representing 8 work items currently in WG process
Documents in IESG

• Subject public key info parameters
  – Elliptic Curve Cryptography Subject Public Key Information (ecc-subpubkeyinfo-09)
    • Status: In AD Review
  – Update for RSAES-OAEP Algorithm Parameters (rfc4055-update-01)
    • Status: Publication Requested
# 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-05</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Trust Anchor Management</td>
<td>ta-mgmt-reqs-02</td>
<td>Standards Track</td>
</tr>
<tr>
<td></td>
<td>cms-content-constraints-00</td>
<td>(Informational Requirements)</td>
</tr>
<tr>
<td></td>
<td>tamp-00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ta-format-00</td>
<td></td>
</tr>
<tr>
<td>Clearance Attribute and Clearance Constraints</td>
<td>authority-clearanceconstraints-00</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Attribute Certificate Profile Update</td>
<td>3281update-01</td>
<td>Standards Track</td>
</tr>
<tr>
<td>New ASN.1 Modules for PKIX</td>
<td>new-asn1-01</td>
<td>Standards track</td>
</tr>
<tr>
<td>Traceable Anonymous Certificate</td>
<td>tac-01</td>
<td>Experimental</td>
</tr>
<tr>
<td>PKI Resource Query Protocol (PRQP)</td>
<td>prqp-00</td>
<td>Experimental</td>
</tr>
<tr>
<td>Other Certs Extension</td>
<td>other-certs-01</td>
<td>Experimental</td>
</tr>
</tbody>
</table>