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

July 30, 2008 1300 - 1500
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 72nd IETF in Dublin

• Introduction
  – Document Status Overview

• WG documents
  – 3279/4055 Update, Sean Turner
  – New ASN.1 Modules for PKIX, Jim Schaad
  – Trust Anchor Management (TAM), Carl Wallace
  – Traceable Anonymous Certificate (TAC), SangHwan Park
  – PKI resource Query Protocol, Massimiliano Pala
  – Other-certs extension, Stephen Farrel

• Related specifications and Liaison
  – OCSP Algorithm Agility, Phil Hallam-Baker
  – Clearance and CA Clearance Constraints, Sean Turner
Status since last meeting

- 4 New RFCs published
- 0 documents in IESG
- 8 drafts currently in WG process
Published RFCs

- Certificate and CRL profile
  - RFC 5280

- CMC
  - RFC 5272
  - RFC 5273 (Transport protocols)
  - RFC 5274 (Compliance Requirements)
# WG Documents

<table>
<thead>
<tr>
<th>Work item</th>
<th>File</th>
<th>Intended status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Algorithms and Identifiers for DSA and ECDSA</td>
<td>draft-ietf-pkix-sha2-dsa-ecdsa-04</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Elliptic Curve Cryptography Subject Public Key Information</td>
<td>draft-ietf-pkix-ecc-subpubkeyinfo-06</td>
<td>Standards Track</td>
</tr>
<tr>
<td>Trust Anchor Management Problem Statement</td>
<td>draft-ietf-pkix-ta-mgmt-problem-statement-01</td>
<td>Informational</td>
</tr>
<tr>
<td>Trust Anchor Management Requirements</td>
<td>draft-ietf-pkix-ta-mgmt-reqs-00</td>
<td>Informational</td>
</tr>
<tr>
<td>New ASN.1 Modules for PKIX</td>
<td>draft-ietf-pkix-new-asn1-01</td>
<td>Standards track</td>
</tr>
<tr>
<td>Update for RSAES-OAEP Algorithm Parameters</td>
<td>draft-ietf-pkix-rfc4055-update-01</td>
<td>Standard Track</td>
</tr>
<tr>
<td>Traceable Anonymous Certificate</td>
<td>draft-ietf-pkix-tac-00</td>
<td>Informational / Experimental</td>
</tr>
<tr>
<td>PKI Resource Query Protocol (PRQP)</td>
<td>draft-ietf-pkix-prqp-00</td>
<td>Experimental</td>
</tr>
</tbody>
</table>