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

March 10, 2008 0900 - 1130

PKIX WG (pkix-wg)

- Web page: charter, current documents
  - http://www.ietf.org/html.charters/pkix-charter.html
- 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
  - Sam Hartman hartmans@mit.edu

PKIX Agenda for 70th IETF

- Introduction
  - (09:00) Document Status Overview
- WG documents
  - (09:05) 3279/4055 Update
  - (09:15) New ASN.1 Modules for PKIX
  - (09:30) TA Requirements
- Related specifications and Liaison
  - (09:50) Wildcards in DNS Names
  - (10:00) PKI Resource Query Protocol (PRQP)
  - (10:10) Other Certificates Extension
  - (10:20) Traceable Anonymous Certificate Protocol
  - (10:30) PKIX Considerations for Usable Security
  - (10:35) Clearance and CA Clearance Constraints
  - (11:00) Open discussion

Status Review

- 1 documents approved
- 3 documents in IESG
- 1 Document Expired
- 4 new documents in WG process

Approved Documents

- RFC 3280bis
  - In RFC editors queue

In IESG (various stages)

- CMC (3 documents)
  - New ID needed. 1 final clarifying text remains to be crafted.

Expired Drafts

- Draft for ECDSA and DSA with SHA-2 family of hash algorithms
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-sha2-dsa-ecdsa-01.txt

4 New WG Documents

- ECC Subject Public Key Info
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-ecc-subpubkeyinfo-03.txt
- RFC 4055 Update
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc4055-update-00.txt
- TA Management problem statement
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-ta-mgmt-problem-statement-01.txt
- New ASN.1 Modules for PKIX
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-asn1-00.txt