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

November 18, 2008 1520 - 1720

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
  - Pasi Eronen pasi.eronen@nokia.com

PKIX Agenda for 72nd 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

Work item	Drafts (draft-ietf-pkix-)	Intended status
Additional Algorithms and Identifiers for DSA and ECDSA	sha2-dsa-ecdsa-05	Standards Track
Trust Anchor Management	ta-mgmt-reqs-02 cms-content-constraints-00 tamp-00 ta-format-00	Standards Track (Informational Requirements)
Clearance Attribute and Clearance Constraints	authorityclearanceconstraints-00	Standards Track
Attribute Certificate Profile Update	3281update-01	Standards Track
New ASN.1 Modules for PKIX	new-asn1-01	Standards track
Traceable Anonymous Certificate	tac-01	Experimental
PKI Resource Query Protocol (PRQP)	prqp-00	Experimental
Other Certs Extension	other-certs-01	Experimental