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

March 23, 2009 - 0900

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 stefan@aaa-sec.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
  - PKI Resource Query Protocol, Massimiliano Pala
  - Traceable Anonymous Certificate (TAC), SangHwan Park
  - Trust Anchor Management (TAM), Carl Wallace
  - OCSP Algorithm Agility, Phil Hallam-Baker
  - Time-Stamp Protocol update, ? OBO Denis Pinkas
  - Advance RFC 5280 to Draft, David Cooper
  - New ASN.1 for PKIX, Jim Schaad
  - Algs and identifiers for DS and ECDSA, Quynh Dang?
- Related specifications and Liaison
  - NSA's Suite B Certificate and CRL Profile, Lydia Zieglar
  - Visual representation of Certificate based eID, Stefan Santesson

Status since last meeting

- 1 New RFCs published
  - RFC 5480, Elliptic Curve Cryptography Subject Public Key Information
- 1 document in RFC Editor's Queue
  - Update for RSAES-OAEP Algorithm Parameters (rfc4055-update-02)
- 0 documents in IESG
- 12 drafts representing 8 work items currently in WG process

Active WG Documents

Work item	Drafts (draft-ietf-pkix-)	Intended status
Additional Algorithms and Identifiers for DSA and ECDSA	sha2-dsa-ecdsa-06	Standards Track
Trust Anchor Management	ta-mgmt-reqs-03 tamp-01 ta-format-01	Standards Track (Informational Requirements)
Clearance Attribute and Clearance Constraints	authorityclearanceconstraints-01	Standards Track
Attribute Certificate Profile Update	3281update-04	Standards Track
New ASN.1 Modules for PKIX	new-asn1-03	Standards track
Traceable Anonymous Certificate	tac-02	Experimental
PKI Resource Query Protocol (PRQP)	prqp-02	Experimental ?
Other Certs Extension	other-certs-02	Experimental
Time Stamp Protocol Update	Rfc3161bis-01	Standards Track
OCSP Algorithm Agility	Ocspagility-00	Standards Track