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

July 26, 2007 1510 - 1610

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 69th IETF

- Introduction
  - (15:10) Document Status Overview
- WG documents
  - (15:15) SCVP
  - (15:20) Subject Public Key info for ECC keys
- Related specifications and Liaison
  - (15:25) WebDav for certificate publication and revocation
  - (15:35) SCEP
  - (15:45) PRQP
  - (15:50) Syntax for binding documents with time-stamps
  - (15:55) Framework on key compromise
  - (16:00) Three short fixes
  - (16:05) Discussions

Status Review

- 2 documents approved
- 5 documents in IESG
- 1 documents in WG process
- 1 Document expired

Approved Documents

- Lightweight OCSP (Proposed Standard)
  - In RFC editors queue
- Service Name SAN
  - In RFC editors queue

In IESG (various stages)

- Server-based Certificate Validation Protocol (SCVP)
  - In AD followup
- RFC 3280bis
  - In AD evaluation
- CMC (3 documents)
  - In AD evaluation : Revised ID needed

Drafts in WG process

- Draft for ECDSA and DSA with SHA-2 family of hash algorithms
  - Was blocked on NIST publication of FIPS 186-3
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-sha2-dsa-ecdsa-01.txt

Expired drafts

- ECC algorithms
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-ecc-pkalgs-03.txt

Draft Anouncement

- Credential Selection Criteria Data Structure
  - http://www.ietf.org/internet-drafts/draft-santesson-credsel-00.txt
- Information model for exchanging credential preferences over various protocols.