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

December 03, 2007 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
  – Sam Hartman hartmans@mit.edu
PKIX Agenda for 70th IETF

• Introduction
  – (13:00) Document Status Overview

• WG documents
  – (13:05) 3280bis
  – (13:10) Subject Public Key info for ECC keys
  – (13:25) CMC
  – (13:30) OCSP Algorithm agility

• Related specifications and Liaison
  – (13:40) Liaison statements received from ITU-T SG17
  – (13:50) Trust Anchor Management (TAM)
  – (14:20) Updating ASN.1 modules to 1998 syntax
  – (13:30) Credential selection - Mainly a PKI problem
  – (13:40) Resource Discovery Protocol
  – (13:50) Discussions
Status Review

- 1 documents approved
- 4 documents in IESG
- 1 documents in WG process
- 1 Document expired
Approved Documents

• SCVP
  – In RFC editors queue
In IESG (various stages)

- RFC 3280bis
  - In IETF last call
- CMC (3 documents)
  - In IETF last call and WG reconfirm requested by AD: Revised ID posted
Drafts in WG process

• Draft for ECDSA and DSA with SHA-2 family of hash algorithms
Expired drafts

• ECC algorithms