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

November 10, 2009 1300-1500

IETF 76 - Hiroshima

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 76th IETF in Hiroshima

- Introduction
  - Document Status Overview, Stefan Santesson
- WG documents
  - Trust Anchor Management (TAM), Carl Wallace
  - OCSP Algorithm Agility, Stefan Santesson
  - Time-Stamp Protocol update, Stefan Santesson
  - Certificate Image, Stefan Santesson
- Related specifications and Liaison
  - RFC 5280 Implementation report, Tim Polk
  - Certificate Information Expression, Stefan Santesson
  - Attribute certificates for XMPP, Sean Turner
  - Proxy Architecture on DRM Service, Zhipeng Zhou

Status since last meeting

- 2 New RFCs published
- 4 documents in RFC Editor's Queue
- 4 documents in IESG processing
- 7 drafts representing 6 work items currently in WG process

New RFCs Published

- RFC 5636
  - Elliptic Curve Cryptography Subject Public Key Information
- RFC 5697
  - Other Certificates Extension

RFC Editor's Queue

- Update for RSAES-OAEP Algorithm Parameters
  - draft-ietf-pkix-rfc4055-update-02
- Attribute Certificate Profile - 3281bis
  - draft-ietf-pkix-3281update-05
- Additional Algorithms and Identifiers for DSA and ECDSA
  - draft-ietf-pkix-sha2-dsa-ecdsa-10
- Trust Anchor Format
  - draft-ietf-pkix-ta-format-04

In IESG process

- In IETF Last Call
  - The application/pkix-attr-cert Content Type
    - draft-ietf-pkix-attr-cert-mime-type-02
  - New ASN.1 Modules for PKIX
    - draft-ietf-pkix-new-asn1-07
  - ESSCertIDv2 update for RFC 3161
    - draft-ietf-pkix-rfc3161-update-09
- Waiting for AD Go-Ahead
  - Clearance Attribute and Authority Clearance Constraints
    - draft-ietf-pkix-authorityclearanceconstraints-02

Active WG Documents

Work item	Drafts (draft-ietf-pkix-)	Intended status
Trust Anchor Management	ta-mgmt-reqs-04 tamp-04	Standards Track (Informational Requirements)
OCSP Algorithm Agility	ocspagility-03	Standards Track
Certificate Image	certimage-01	Standards Track
Transport Protocols for CMP	cmp-transport-protocols-07	Standards Track
PKI Resource Query Protocol (PRQP)	prqp-03	Experimental
ASN.1 Translation	asn1-translation-00	Informational