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

March 27, 2012 0900-1130

IETF 83 - Paris

PKIX WG (pkix-wg)

- Web page: charter, current documents
  - http://datatracker.ietf.org/wg/pkix/charter/
- Mailing List: pkix@ietf.org
    - To Subscribe: pkix-request@ietf.org
    - Archive: http://www.ietf.org/mail-archive/web/pkix/
- Chairs
  - Stephen Kent kent@bbn.com
  - Stefan Santesson stefan@aaa-sec.com
- Security Area Director
  - Sean Turner turners@ieca.com

PKIX Agenda for 83th IETF in Paris

- Introduction
  - Document Status Overview, Stefan Santesson
- WG documents
  - RFC2560bis, Stefan Santesson
    - Issues with RFC2560 and RFC2560bis, Denis Pinkas
  - Enrollment over Secure Transport, Max Pritikin
  - Diffie-Hellman Proof-of-Possession Algorithms, Jim Schaad
- Related specifications and Liaison
  - Certificate revocation for high volume websites, Max Pala
  - Security policy flag 'Must be OCSP stapled', Phil Hallam-Baker
  - ClaimSgining EKU, Matt King
  - Authentication context QCStatement, Stefan Santesson
  - OCSP ’Not Issued’ statement, Denis Pinkas

Status since last meeting

- 1 New RFCs published
- 0 documents in RFC Editor's Queue
- 1 documents in IESG processing
- 6 drafts currently in WG process

New RFCs published

- RFC 6402 – November 2011
  - Certificate Management over CMS (CMC) Updates

In IESG Processing

- AD Evaluation::Revised ID Needed
  - draft-ietf-pkix-cmp-transport-protocols-16

Active WG Documents

Work item	Drafts (draft-ietf-pkix-)	Intended status
Clarifications to RFC 5280	rfc5280-clarifications-04	Expired (ST)
OCSP update	rfc2560bis-04	Standards Track
S/MIME capabilities for pub keys	pubkey-caps-04	Standards Track
DNS CA authorization resource record	caa-05	Standards Track
CMC server key generation	cmc-serverkeygeneration-00	Standards Track
Enrollment over secure transport	est-01	Standards Track