

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

March 22, 2010 1520-1720

IETF 77 - Anaheim

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 77th IETF in Anaheim

- Introduction
 - [Document Status Overview](#), Stefan Santesson
- WG documents
 - [Trust Anchor Management \(TAM\)](#), Carl Wallace
 - [ASN.1 Translation](#), Carl Wallace
 - [Progression of RFC 5280](#), David Cooper
 - [Certificate Image](#), Stefan Santesson
- Related specifications and Liaison
 - [Suite B Profile for CMC](#), Sean Turner
 - [Revocation info extension](#), Magnus Nyström
 - [Revocation by key identifier](#), Magnus Nyström
 - [Application Server Identity](#), Peter Saint-Andre
 - [CertID and KeyID for PKIX](#), Sean Leonard
 - [\(Proxy Architecture on DRM Service\)](#), Zhipeng Zhou)

Status since last meeting

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

New RFCs Published

- RFC 5758
 - Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA
- RFC 5755
 - An Internet Attribute Certificate Profile for Authorization (obsoletes RFC 3281)
- RFC 5756
 - Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters

RFC Editor's Queue

- MIME Media Type for Attribute Certificates
 - [draft-ietf-pkix-attr-cert-mime-type-03](#)
- ESSCertIDv2 update for RFC 3161
 - [draft-ietf-pkix-rfc3161-update-09](#)
- Trust Anchor Format
 - [draft-ietf-pkix-ta-format-04](#)
- New ASN.1 Modules for PKIX
 - [draft-ietf-pkix-new-asn1-07](#)

In IESG process

- Publication requested
 - OCSP Algorithm Agility
 - [draft-ietf-pkix-ocspagility-08](#)
- IESG Evaluation
 - Trust Anchor Management Protocol
 - [draft-ietf-pkix-tamp-09](#)
- Approved
 - Clearance Attribute and Authority Clearance Constraints
 - [draft-ietf-pkix-authorityclearanceconstraints-02](#)

Active WG Documents

Work item	Drafts (draft-ietf-pkix-)	Intended status
Certificate Image	certimage-01	Standards Track
Trust Anchor Management	ta-mgmt-reqs-04 tamp-04	Standards Track (Informational Requirements)
PKI Resource Query Protocol (PRQP)	prqp-03	Experimental
ASN.1 Translation	asn1-translation-00	Informational
<i>Rogue drafts</i>		
CertID and KeyID for PKIX	certid-keyid-01	Non WG
Transport Protocols for CMP	cmp-transport-protocols-07	Non WG