

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

July 29, 2009 1300-1500

IETF 75 - Stockholm

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 75th IETF in Stockholm

- 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
 - [Algs and identifiers for DS and ECDSA](#), Tim Polk
- Related specifications and Liaison
 - [Certificate Information Expression](#), Stefan Santesson
 - [Relying party software tool development for SIDR](#), Stephen Kent

Status since last meeting

- 0 New RFCs published
- 3 documents in RFC Editor's Queue
- 3 new documents in IESG
- 9 drafts representing 8 work items currently in WG process

RFC Editor's Queue

- Update for RSAES-OAEP Algorithm Parameters (rfc4055-update-02) – waiting for 3281bis
 - [draft-ietf-pkix-rfc4055-update-02](#)
- Attribute Certificate Profile - 3281bis
 - [draft-ietf-pkix-3281update-05](#)
- Traceable Anonymous Certificate
 - [draft-ietf-pkix-tac-04](#)

In IESG process

- In IETF Last Call
 - Clearance Attribute and Authority Clearance Constraints
 - [draft-ietf-pkix-authorityclearanceconstraints-02](#)
 - Other Certificates Extension
 - [draft-ietf-pkix-other-certs-04](#)
- Scheduled for telechat August 13
 - Trust Anchor Format
 - [draft-ietf-pkix-ta-format-03](#)

Active WG Documents

Work item	Drafts (draft-ietf-pkix-)	Intended status
Additional Algorithms and Identifiers for DSA and ECDSA	sha2-dsa-ecdsa-06	Standards Track
Trust Anchor Management	ta-mgmt-reqs-03 tamp-02	Standards Track (Informational Requirements)
New ASN.1 Modules for PKIX	new-asn1-05	Standards track
PKI Resource Query Protocol (PRQP)	prqp-03	Experimental
Time Stamp Protocol Update	rfc3161bis-01	Standards Track
OCSP Algorithm Agility	ocspagility-00	Standards Track
Certificate Image	certimage-00	Standards Track
ASN.1 Translation	asn1-translation-00	Informational