

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

July 25, 1300-1500

IETF 81 – Quebec, CA

# PKIX WG (pkix-wg)

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

# PKIX Agenda for 81<sup>st</sup> IETF in Quebec

- Introduction
  - [Document Status Overview](#), S. Kent
- WG documents
  - [DNS Certification Authority Authorization \(CAA\) Resource Record](#), P Hallam-Baker)
  - [CAA Comments](#), P. Hoffman
- Related specifications and Liaison
  - [Enrollment over Secure Transport](#), M. Pritkin
  - [CMC Extensions: Server Side Key Generation & Key Escrow](#), S. Turner

# Status since last meeting

- 2 New RFCs published
- 0 documents in RFC Editor's Queue
- 0 documents in IESG processing
- 7 drafts currently in WG process
- 1 draft likely to be adopted?

# New RFCs Published

- RFC 6170
  - [Internet X.509 Public Key Infrastructure -- Certificate Image](#), 2011-05
- RFC 6277
  - [Online Certificate Status Protocol Algorithm Agility](#), 2011-06

# Active WG Documents

| <b>Work item</b>  | <b>Drafts (draft-ietf-pkix-)</b>           | <b>Intended status</b> |
|---|--|------------------------|
| CMC Updates   | <a href="#">rfc5272-bis-01</a>             | Standards Track        |
| Clarifications to RFC 5280                              | <a href="#">rfc5280-clarifications-01</a>  | Standards Track        |
| OCSF update   | <a href="#">rfc2560bis-02</a>              | Standards Track        |
| Transport Protocols for CMP                             | <a href="#">cmp-transport-protocols-13</a> | Standards Track        |
| DNS Certification Authority Authorization RR            | <a href="#">caa-01</a>                     | Standards Track        |
| Internationalized Email Addresses in X.509 certificates | <a href="#">eai-addresses-00</a>           | Standards Track        |
| S/MIME Capabilities for Public Key Definitions          | <a href="#">pubkey-caps-02</a>             | Informational          |