PKIX WG Meeting March 12, 2013

Edited by Steve Kent
Co-Chairs: Stephen Kent <kent@bbn.com>
Stefan Santesson <stefans@aaa-sec.com>

The PKIX WG met once, during a 1.5 hour time slot, during IETF 86, in Orlando, FL. A total of approximately 49 individuals attended the meeting.

Document Status Review – Stefan Santesson (3xA)
There has been progress in document status since November, 2012.
- 2 new RFCs: Update to 5280 (6818), DNS CAA (6844)
- 1 document in IESG evaluation (2560bis)
- 1 active I-D in the WG: EST (-05)
(Slides)

The Future of PKIX – Sean Turner (IECA)
Sean reiterated his plan to complete the orderly shutdown of PKIX. He says this is expected to be the last meeting of PKIX, which began in 1995. The WG list will remain open. (no slides)

PKIX WG Document

Enrollment over Secure Transport (EST) – Max Pritikin (Cisco)
Max described changes since the -04 version. He noted that there was a lot of helpful comments on the -05 version, which is causing changes that will result in an -06 version, which he is working on now. Improvements include substantial prose improvements, explicit vs. explicit TA terminology, use of well-know UIRs. For the -065 version, the authors will fix the MIME representations, to remove the PEM headers, and they will include improved security for server-side generation exchange. It was reported that there are now two independent implementations that interoperate, which would allow the document to move very quickly to full standard status. (Slides)

Non-WG Topic Presentation

Authentication Context Extension – Stefan Santesson (3XA)
This proposal describes an X.509 certificate extension that can be used by an RP to help map subject identity info, in a federated identity management environment based on the use of SAML. Stefan provided examples based on European PKI deployments, which motivate this work. The extension makes use of XML, because that is the native encoding for SAML assertions. Stefan’s slides included detailed examples. This is an independent submission. (Slides)