PKIX WG Meeting November 8, 2012

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

The PKIX WG met once, for 1 hour during IETF 85, in Atlanta, GA. A total of approximately 30 individuals participated in the meeting.

Document Status Review – Stefan Santesson (3xA Security)

There has been some progress in document status since August.

- 1 New RFC (RFC 6712 – HTTP transfer for CMP)
- 1 document in RFC Editor's queue (RFC 5280 clarifications)
- 1 document in IESG processing (DNS CAA Resource Records)
- 2 drafts currently in WG process (RFC2560bis and EST)
- 1 expired WG draft (CMC Server Key Generation)

(Slides)

The Future of PKIX – Sean Turner (IECA)

Sean informed about the orderly shutdown of PKIX. To this end he doesn't want to accept any new work items. He wants the current last active WG documents to be finalized by March 2013.

PKIX WG Documents

Enrollment over Secure Transport (EST) – Peter Yee (AKAYLA)

A new draft (03) has been submitted since last IETF, dealing with all comments received on the 02 draft. The changes includes new explanatory text, clarification of document intent, added support for "certificate-less" cipher suites in TLS and updates to the Security Considerations section. Comments on the 03 draft has been received from Stephen Kent who has expressed several issues with explanations and descriptions in the draft. An updated 04 draft is currently being prepared as response to the review by Steve Kent. This will include a new terminology list, separated tables for certificates and trust anchors and more consistent RFC2119 language. The new draft will be posted on November 26.
Sean Turner suggested using alternate language for lower case must/should/may words.

Sean Turner has requested an early Apps review of this document. He will get back in two weeks with more information.
(slides)

CMC Server Key Generation – Sean Turner (IECA)

This document has stalled due to disagreements among the authors on how to resolve previous comments. Sean will investigate whether this document can be finalized within PKIX or whether it will be allowed to die, or alternatively be processed outside of PKIX. There is a reference dependency where the EST draft references this draft. This might be an issue for the finalization of the EST draft. Sean Turner declared that this document shall not hold up the WG closure.

RFC2560bis (OCSP Update) – Stefan Santesson (3xA Security)

This document has been updated since last IETF (draft 06). Updates includes clarification of the responderID field, inclusion of original authors of OCSP, expansion of the revoked response to allow revoked as response to status requests for non-issued certificates and updates to the definition of Authorized responders. A major discussion on the list has explored the proposal to expand the revoked response. The WG recently held a straw-poll with a strong majority favoring the proposed expanded definition if is complemented by a new empty and non-critical extension declaring that the responder operates according to the new expanded definition of “revoked”. A major question to the group is whether the new extension MUST be included in all responses or just when responding to non-issued certificates.
Phil Hallam Baker said that he want’s to be able to declare ranges in the new extension but agreed that this should be a task for a separate extension.
Scott expressed concern about the certificateHold status since CAB Forum may hare requirements to never use certificateHold status when revoking certificates. This will probably not be an issue since this status is not applied to revocation of issued certificates.
Sean Turner suggested that we should test this through real implementation and see if anything breaks. This could probably be done rather fast.
Carl Wallace asked why we would not put an EKU in the OCSP responder cert.

Phil Hallam Baker responded that some OCSP servers issues responses directly off the CA cert. Adding EKU is not possible or problematic in such cases. Phil wandered further why we need an extension at all.
Russ Hously responded that we need the extension to allow auditing of OCSP performance against operational policies.
The meeting concluded unanimously to support the proposed resolution on the use of “revoked” status for non-issued certs with a MUST requirement to include the new extension when responding “revoked” to non-issued certificates and that OCSP responders MAY include the extension in all responses.
(slides)

Open Mike:

Phil Hallam Baker: Informed that he is writing a staple draft that defines an extension for inclusion in server certificates that informs TLS clients that this server always offers OCSP stapling in TLS. Current draft 02 is out and draft 03 will be published soon.