PKIX WG Meeting March 26, 2012

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

The PKIX WG met once, for 2.5 hours, during IETF 83, in Paris. A total of approximately 52 individuals participated in the meeting.

Document Status Review – Stefan Santesson (3xA)

There has been significant progress in document status since the previous meeting.

- 1 new RFC published since Prague (6402)
- 1 document in IESG processing (CMP transport protcols)
- 7 active I-Ds in the WG: CMC Updates (EST, 5280 clarifications, OCSP Update, Transport Protocols for CMP, S/MIME Capabilities for public keys, CMC server key generation, CAA)

(Slides)

PKIX WG Documents

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

The I-D is has been stalled but Stefan expressed confidence that this document can make progress now. The major problem has been the text clarifying how (authorized) responders should behave, not format changes to the protocol. Stefan argues that text proposed in this document will not work well, because it does not match how many OCSP responders and clients have been implemented. He suggests several changes designed to better match widely deployed responder and client practices, via clarifications. At the microphone there was one expression of support and one expression of concern for the proposed changes. (Slides)

Issues with RFC 2560 and 2560bis - Denis Pinkas (Bull SAS)

Denis argues that OCSP is reasonably well specified for simple cases, but even in this case he says there are some missing details, e.g., re appropriate KeyUsage bits in an OCSP responder certificate. In more complex cases he feels that the (original) document is under-specified. The central issue here the burden on clients re determining whether a given OCSP responder is authorized to reply for a given target certificate. Denis expressed concern that the status of Appendix E (in 2560bis) is not clear; he feels it is normative. He also feels that 2560bis should provide a clearer description of the verification process that an OCSP client will follow. Denis's slides provide details of edits he believes need to be performed, while maintaining compatibility with RFC 2560. He identified several apparent errors in the current text, e.g. references to OCSP supporting queries for certificates in the "distant past." Stefan expressed support for many of Denis's comments. Sean urged Stefan to complete work on this later this year. (Slides)

Enrollment over Secure Transport (EST) – Peter Yee (AKAYLA) and Max Pritkin (cisco)

Peter noted that the current draft is much changed since the -01 draft. He provided an overview of EST. The protocol employs TLS channel binding in support of PoP. HTTP client authentication is a fallback, but client side certificates with HTTPS is preferred. EST includes a feature to support distribution of current root CA (TA) and rollover of a TA certificate. EST uses SIMPLE CMC messages for enrollment and re-enrollment (certificate renewal). However, there is also full CMC support as an option, for contexts where SIMPEL CMC messages do not suffice. A newly added feature is support for serer-based key pair generation, a feature requested to support uses cases in the SIDR WG.

Max described his current implementation of EST, and noted that there are 3 implementations in progress.(This is not intended to be a production-quality implementation.) This implementation will be made available on an open source implementation. It could become a reference implementation in the future. Max described the components he used for his implementation, including mongoose, OpenSSL, etc. Max noted which features are present and which still need to be completed. Paul Hoffman asked if EST has become focused more on provisioning certificates to servers vs. clients? Max says no; use of TLS_UNIQUE is not intended to convey this notion. Use of

TLS_UNIQUE is optional. (Slides)

Diffie-Hellman Proof-of-Possession Algorithms, Jim Schaad (August Cellars)

Jim noted that the original document described two methods of computing a "signature" using Diffie-Hellman: key agreement + HMAC-SHA1 and a discrete log signature (DSA-like). The intent of this revision is to parameterize the description in support of algorithm agility, e.g., to accommodate SHA-256 and SHA-512 and for Elliptic Curve Diffie-Hellman. This is a proposed update to RFC 2875, so it is not, technically a WG item yet. Steve Kent asked Jim to request formal WG adoption in the list. Sean Turner said that he would be happy to sponsor this as an individual document if the WG does not elect to adopt it. (Slides)

RFC5280 Clarifications

This topic was added at the beginning of the meeting, at Paul Hoffman's request. David Cooper, the document author was not present. Paul suggests that we work on the list to revise the text dealing with self-signed end-entity certificates, as the primary, remaining open issue for this document. Steve Kent agreed to work with Paul on revised text on this topic. (no slides)

Presentations on non-WG Topics (seeking WG adoption)

Certificate revocation for high volume websites Massimiliano Pala (NYU)

This presentation is motivated by the various TLS trust model problems that motivated some of the DANE work, the IAB technical plenary discussion yesterday, and various browser modification proposals. Max briefly reviewed several of these efforts: DANE, certificate pinning, "perspectives," "convergence," MECAI, and "sovereign keys." Max is working to develop comparisons of these proposals, to make it easier to evaluate these proposals. Because some proposals are not completely specified, this may be very difficult. Some aspects of this analysis might be relevant to the ongoing OCSP extensions discussion in PKIX. Max

described various other revocation status distribution approaches, e.g., use of DNS, white lists for CAs (not be confused with certificate white lists issued by a CA), and a new notion for a lightweight revocation token (which Max may pursue via an I-D). Denis argued that, despite citing the problem of a flat trust model in browsers, the presentation seems to assume perpetuation of this "broken" trust model. It also was suggested that short-lived certificates would help with this problem as well. It also was noted that there are other options being pursued, that were not included in Max's presentation. (Slides)

Security policy flag 'Must be OCSP stapled' - Phil Hallam-Baker (Comodo)

Phillip was not able to attend and we were not able to arrange for a remote presentation. (Slides)

ClaimSgining EKU (draft-king-pkix-claimsigning-extn-03.txt) – Pat Patterson (Carillon Information Security)

The proposed EKU is intended to signal that the certificate holder is authorized to sign "claims" (attributes) about a subject. Pat says that this EKU is needed because most servers are issued certificates (by commercial CAs) containing the ServerAuth EKU. But some servers are signing other objects, not just using a server certificate for TLS. The concern is that client might reject signed objects due to strict interpretation of the ServerAuth EKU. The principle cited use case is that of a secure token service that signs SAML assertions. Attribute authorities are also cited as a use case, but this seems questionable, given extant PKIX AA standards. The big issue here is that this is a proposal to solve a problem created by commercial CAs, which will not work unless these CAs agree to issue server certificates with this new EKU. There was some agreement that this does not appear to be a topic for PKIX, and so an individual submission may be appropriate, so long as the resulting topic does not conflict with PKIX RFCs or work in progress. Steve Kent agreed to bring this topic to the list, for resolution. (Slides)

Authentication context Qualified Certificate Statement - Stefan Santesson (3xA Security)

This presentation addresses an analogous issue re SAML assertions. The focus is how to bind certificates and SAML assertions. Stefan described a e-Government use case from Sweden that motivated exploring this topic. In that example users don't have individual certificates. Instead they interact with central signing services that can signature docs on behalf of users, after authenticating them. (It does this by creating a one-shot certificate on behalf of the user, signs the document in question, and then destroys the private key.) Stefan asks whether we might amend RFC 3739 (Qualified Certificates) to try to address this issue. An audience member suggested interacting with OASIS on this topic, since they manage SAML. (Slides)

OCSP "not issued" and RFC 2560 – Denis Pinkas (Bull SAS)

Denis's presentation reviews the current WG list discussion on extending OCSP to reply with a "not issued" status. Part of his presentation suggests that a clause in 2560 might be used to signal whether the OCSP responder is has direct access to a CA database (vs. using a CRL to generate replies). He suggests that if the CA HSM has been used to issue certificates not under the control of the CA, then the CA key MUST be revoked, i.e., no other solution approaches are viable. For a forged certificate with a known serial number, which may overlap with a legitimate certificate, Denis suggests including the certificate hash in the response. Denis believes this can be effected via an extension, without moving to OCSPv2. He suggests maintaining the current, three status values, but adding a secondary status of "not-issued" in a non-critical extension. The presentation concluded with discussion of the efficacy of this approach, noting the attack contexts in which it works and does not work. Stefan noted that he was not convinced that OCSP fixes would solve the broken CA problems that motivated this discussion. (Slides)

SCVP – Denis Pinkas (Bull SAS)

Denis said that he is not surprised that SCVP has not been more widely deployed, given it's complexity, He suggested that a lightweight alternative to SCVP might be more successful. LCVP was the name for this alternative, several years ago, when SCVP was developed. Dens suggests that the WG consider revisiting LCVP at this stage. (no slides)