MD WG 2013-08-29

Present: Ian Young, Harry Nicholos, Mark Scheible, Scott Cantor, John Krienke, IJ Kim, Tom Scavo, Don Faulkner, Nate Klingenstein

---
Phase 1 Report Draft Discussion

AI John will remove the original draft page (a duplicate).

Section: Lifetime of the Current Signing Key.

Need to make it clear there are two issues. First the lifetime of the signing key. Second, the issue of the signing certificate.

Section: Observations.

Clean up the last sentence of the observations, which was truncated. Needs to say something like "... real-time validation of entity lookups with minimal time caching." Also... Expiration date on the OCSP response is very brittle due to expiration date, which is not the case with cache duration in SAML.

Section: Recommendations.

Bullet "Communicate with known users":
Users of the non standard software implementations. Some hesitation about the precedent of being so hands-on with other implementations. If we have to support a broad set of implementations, we're setting ourselves up for a resource commitment and investment. Good customer service yes, but with people using unsupported software the drain could be significant. Communicating with (Microsoft, SimpleSAML) developers is a different matter – one we should do. So, clarify what we mean by Communication vs Support. TAC may want to use this as a point in time to review the software guidance page. Also discussed the goodness of documenting implementation issues – might have a lot of push back from vendors whose software might be cast as deficient. Where is the right place to make objective claims about non compliance – the federation or Shib website? Shib might be a more objective player. Objective statements will be key: "Does not implement" "does not support" etc. rather than broken.

Bullet "Expired Certificates."
Make it clear that we don't see the issues coupled with issues on the MD signing key. They really are not coupled. The certs in MD were never intended to be evaluated in the context of the CA. It /is/ a separate matter. CA needs at the time might have been more around controlling key lifetime. Shib didn't generate certificates early in its development.

Bullet "Resign the same key."
Specific validity period? A re-key is the specific event of consideration. Could be helpful to look across CAs to make a determination on what a key lifetime of a CA should be. A certificate's expiration may be less about to a key's lifetime than the notion of when a key should be reevaluated. We're really saying the validity period of a new self-signed certificate wrapped around the existing signing key is a promised evaluation period. At the end of the validity period, we may re-key or not, depending on another security evaluation. However, evaluation is always an ongoing issue. If a vulnerability is discovered we will take immediate action.

Will commercial CA re-keys teach us anything? In all cases Ian has seen in last 4-5 years, the certs have had extremely distant expiry dates. Older Verisign expiry dates were in the 2020s back in 1995. In the case where a CA does reach its expiration date, what typically happened? From client perspective, you have to update or things break. If the root or intermediate expired, the response was to set up an entirely new CA with no relationship with the old, no cross signatures etc.

So, a certificate's Lifetime doesn't mean we won't have to do something sooner. This is the whole point of revocation, and therefore, Revocation strategy is critical to document. AI. We do not expect to make a determination that affects the lifetime of the key anytime soon. Technology developments will affect the strength in the future. Make the recommendation that our cert expire in 2038. Perhaps generate another cert with the same signing key that goes beyond for anyone who wants to test.

Note: this would be a good time to revisit the cert advice on the InCommon cert recommendations page. We toned down the 3 year wording. AI to look at this page as it relates to our own advice above. Recommendation to TAC to look at these bits. Risk is identical (of key exposure).

AI scott to write requirements for ops on per entity md testing.

For documenting templates available for signing keys, Scott did check with Leif. There are no known specs in the works, perhaps use PKI lite. This is the template InCommon used for its CP/CPS of the self-signed CA under discussion.

Action Items

AI John will remove the original draft page (a duplicate).
AI Suggest that TAC/Ops review the Certificates in MD page
AI Scott will initiate requirements for Ops to start testing per-entity MD