MD WG Meeting 2013-07-25

Present: Harry Nicholos, IJ Kim, Tom Scavo, John Krienke, Scott Cantor, Ian Young, Paul Caskey,

AGENDA:

Review Phase 1 Requirements in light of offline and online signing
discussions.

PHASE 1:

- Determine if the current metadata signing key and certificate needs to be replaced or renewed.
- Determine if the key pair requires a traditional PKI.
- Communicate to InCommon participants expectations and any required or recommended actions needed

MINUTES/NOTES: Includes errata sent as of 8 Aug 2013.

Developing Consensus: No strong use case for a PKI, as distinguished from the possible need of an online signing key (which may or may not require a full blown PKI).
HSM is a critical concern for online, but possibly not a CA/PKI.

Related to the second bullet point of Phase 1 above:
Two conditions would affect the need for a new signing key. (1) any attacks known which depend on having large amounts of cypher text available (the more you generate, the more vulnerable you are.) There aren no known attacks of this nature now; and, the amount of known cypher text generated by our signing activities is miniscule.
(2) Sheer computational power. Someone may have been applying resources over the 10 year period of our key's life span. Not practical even with today's technology for a 2048 bit RSA key.

To be written up as draft consensus for this working group's communications:

1. TAC
The Signing key: keep it. re-wrap it in a new self-signed wrapper? Yes, reduces confusion, nothing will break. How long a term should the self-signed cert be? TBD.

Known issues:

Ian knows of software that is sensitive to the expiry of the signing certificate (for example, some of Eduserv's software).

SimpleSAML.php will have a migration problem due to a change in the fingerprint (based on the cert wrapper not just the key). Taking the key info element, extracting ... signature validation of messages is done this way as well (if collisions can be generated). Practically, the longer timeline of the current signing cert's expiration date could be of value (albeit longer than the expiration of the CA root cert). AI Tom will contact SSPHP devs to see about considering this. When we re-wrap our signing cert, it causes sys admins issues. Scott noted that PGP uses key fingerprint rather than cert fingerprint. 20 byte hash of certificate ID. Could use the modulus as the key. Tool to get that. Cert fingerprint is literally a Sha1 of the octet sequence (asn1).

2. Participants
Remind participants if they are relying on the PKI that is there, they're relying on security patterns that are no longer relevant. Low risk with exception of the govt. AI Reach out to the gov on these fronts (NIH, NSF). When was the last expiry of our old InCommon issued certificates? Answer: All are now expired. We'll want to mention the effects to end-entity certs as well. Cert wrapper is irrelevant ... expiration doesn't matter (reminders).

3. New type of policy document to replace the CP/CPS.
IETF activity around a simpler template for PKIs? CP/CPS model too heavyweight. Is there a template model for something like a PKI that isn't? AI Scott will email Leif. Key management may be too down in the technical stack for REFeds. AI John will review what REFeds has on the Federation Policy template front.

NEXT PHASE

Looking at the 5 points of Phase 2.https://spaces.at.internet2.edu/x/zRBOAg

SHA2 is orthogonal but important.

How do we create additional MDAs (metadata aggregates) and the need to be able to test things in the MD before we move to production? For instance, adding other extensions. We do need a plan for how to do this ongoing. What about serious nightmare scenarios where we need an extension and older software releases have bugs? Calls out the need for a persistent testing environment. UK has a production MDA, a fall-back MDA and a test MDA. Any new extensions move into the test mda, with multiple new things at the same time. Gradually transition into the production and then finally into the fallback. Currently UK is signing test with Sha256. Current plan is to sign the production aggregate with RSA+SHA-256 from 7-Aug, with the same signing key, not changing that at the same time. UK is maintaining the signature profile of RSA+SHA-1 on the fallback aggregate for at least 3 months beyond the production transition.

AI InCommon Operations to discuss test and fall back environment.

Further Discussion about other comments:
DNS is UDP based and no practical way to get DNS folks to get our info into it. DNS administrators want no part of this. Most likely way for DNS to come into the picture. Can always do http or DNS as a way to dispatch requests to information for multiple sources of MD.

Interfed as a use case for more future facing discussions: The consensus of the discussion was that the interfed community has enough to chew on with fine tuning the trusted movement of aggregates, import/export, etc. Better to focus on the local distribution context first.

Looking for a use case for driving the future discussion for phase 2: This is more of a federation and software problem as it relates to our trust model. Use cases out of technology considerations (brittleness of batches). Dynamic lookups are more complicated than batches. Is MD like a cert, obtained from an authoirity and signed by itself.
Use case: what problems are we trying to solve? Brittleness. What else? OCSP doomed TLS b/c it's still relying on a thrid party host for lookup.

Accumulated Action Items:

AI Tom will contact SSPHP devs to at least discuss the fingerprint based-on-certificate-wrapper issue
AI For communications, InCommon will want to reach out to our gov agency partners on the upcoming signing cert modifications
AI Scott will check with Leif on any IETF or related standards for addressing key management outside of the CP/CPS model
AI InCommon Operations to discuss test and fall back environment for publishing MDAs.
AI John will review what REFeds has available on the Federation Policy template front.
AI John will draft a concensus for the working group to approve next meeting and conclude its Phase 1 recommendations.