MD WG Meeting 2013-08-15

Present: Mark Scheible, Max Miller, Scott Cantor, Ian Young, Nate Klingenstein, John Krienke, Tom Scavo, IJ Kim

Online Signing

Discussed the business and technical requirements of online signing. Frequency of signing relates to staff requirements as well (for example, for MD validation). Does delivering online signing services mean staff needs to be on hand 24/7 – domain approvals could be handled before automated signing (similar to the InCommon Cert service). Signing with a key on an HSM provides the most flexibility against the risk of exposure of the key.

Domain validation may need to be something we do more systematically. Online signing key solves problems. Might not be sufficient, but will probably be necessary for other things. End of day, frequency is the issue. Ad hoc issue. Online is the only way to do it. No obvious use cases for on demand signing are pressing currently. One could be in the creation of custom aggregates, and then needing to add a MD entity within the federation right now, right away.

Aggregate goes away when you think about DNS. For the local only "hidden" MD entities: You don't hide systems from DNS, but you might not register something in DNS at all. If you aren't using the software features for query, you'll be using aggregates, and they can be pre-computed and subscribed to (the current MDA model). Query (MDX) is the driver for per-entity MD.

Discovery related issues with per-entity MD. Security properties are different here than driving trust decisions for application access. Shib is already moving away from XML toward Java Script friendly discovery.

What would online signing buy us?
1. Frequency
2. Automation (certain kinds of changes to MD could be automated w/o need of human intervention). 2 physical people involved in the InCommon signing process. What is the cost of adding aggregates in this queue? Time spent in offline signing will increase. Signing multiple MDA may not add significant time, however. AI Estimate the cost per signing offline. John.
3. Security. Optimize the validity period of the MDA (right now it stands at two weeks due to business processes around certain times of the year, like the holidays). Shortening the validity period may be – net – more of a security benefit than the loss of any security related to online signing. Optimize for the routine, vs optimize for black swan event.

Flexibility for MDAs. Entity categories could help bundle a MDA for Discovery. Predefined and made available on the regular bases with custom validity windows. We don't need online signing to do predefined MDAs. Can't necessarily predict ahead of time. Worst case is supporting custom entity categories in each Org's own name space. May be isolated cases of value here, but most MDA are people not using query at all, or MDA is being used for a different purpose.

HSM performance can differ quite a bit between the high end to low end.

Query and Per-Entity MD.

SP has been able to do this for quite a while. Just nothing it has to go ask. Chicken and egg. Until it's being used, not easy to predict how easy it is to work. Nice to get some experience prior to shipping the IdP with these same features. Signed XML is the requirement. Not signed JSON.

Ian. One implementation should be around soon. Leif is putting a query back end on the REEP service. Directory of MD files back end then set up as a test target. Also relatively simple to split up a MDA. Web service part of the Shib MDA doesn't exist at this point. Server implementation of this could be implemented in a shel script.

Barrier is not a lot of client side implementations for behavior and performance characteristics. Scott can offer shib.net as an early pilot. Happy to turn this on, on Shibboleth.net. Offering up all participants as http query for all IdPs.

Ian has TERENA funding to help on the REEP project. One of the tasks is to resurrect the specification draft for the MD query protocol through the IETF process (it's there now). ISOC coming up with some of the funds as well.

Policy. Framing a prototype so that Ops can come up with an estimate. AI Scott will put something here. AI Ops discussion here.

Actions

AI John to estimate daily signing costs.
AI Scott to write up some prototype requirements for per-entity MD prototype
AI Ops to discuss capability, feasability