MD WG Meeting 2013-08-08

Present: Tom Scavo, John Bradley, Harry Nicholos, Don Faulkner, Ian Young,

Scott Cantor, Mark Scheible, Paul Caskey, Nate Klingenstein, John Krienke

Phase 1 Discussions

Expired certificates in MD: This is a parallel communication effort that we may not want to

conflate with communication about the signing key issues. Note: CA siteminder and ADFS may also not like expired certs. AI Ops will follow up on expired certs after we communicate about the signing key and CA.

Phase 2 Discussions.

Medium Term Issue. Local Metadata Aggregates.

UARK maintains a local metadata aggregate (MDA) today, and wants to federate services within a state network and looking at how to tier it, for locally, regionally, nationally distributed MD. Many SPs for local-only use but don't want to advertise their existence in the public InCommon MDA. Similar to work InCommon is piloting with CMU on producing local-only MDA for participants.

How would we know which IdPs or SPs we should trust? One option would be Entity Categories like R&S. Tag the interested IdPs and SPs as category tags.

What is the value of a local MDA? Discussion revolved around not so much confidentiality as maintenance and distribution. Shouldn't have to publish every entity into the InC Federation. But the more alike the processes are, the more manageable they become.

Is goal to hide an entity via local MA, or to simply not include in the big public MDA? Two different goals. Entity MD solves this. Batch case solves this by customized local MDAs. To lock down the MDA is harder (presumably by encryption, and this is not the use case of concern voiced by anyone on the call).

How do you move an entity from local, to regional, to national MDA? MDX is

supposed to solve this use case. MDX addresses requirement of not having to fetch MD that you don't need. You never need to fetch what you don't need.

There are people who are concerned about hiding things. Need to make it clear

and frame and clarify that local MDA is not true hiding (i.e., confidentiality) but is more

management related. Not confidential, but rather local. Secrecy is not high on the list of priorities in MDX as written; however, filtering is more the focus.

Consuming Multiple MDAs or a Single MDA:

From the Shib perspective, no intrinsic distinction/preference. Only an operational question.

Probably more convenient as you diverge from Shib to consume 1 rather than 2 MDAs. Paul follows single MDA but no compelling preference. OSU consumes multiple (InCommon + local).

More interesting to think about online use cases. When does signing

occur and how often? Campuses currently have next day delays. OSU signs their local MDA on the fly all the time. Hassle to wait a day for InCommon. OSU doesn't sign, just pushes using rsync. Paul & Harry both publish once daily, with occasional out of cycle, similar to InCommon. Don publishes every 15 minutes with automated signatures (due to fast growth). Local test IdP for testing, production IdP. Both consume the local MDA. Files end up on a web server, pulled down similar to InCommon MDA. OSU has two separate MDAs for non-campus and campus.

Per Entity MD and Online/Offline Signing

How to shape the discussion.

MDX and per entity MD publishing don't necessarily imply online signing. MDX can be seen as an addressing scheme. Per entity could be published once a day, addressed by MDX. Can still do these things w/o dynamic online signing.

Scott mentions performance issues, a good question.

Java based signing program for Shib project -- overhead spinning up a JVM every time

you do a signature. Not good performance. But doesn't relate to architecture. MDX

designed to do things that are not compatible with online signing. Like custom

aggregates on demand with query parameters. Interfed not moving in this direction with custom queries.

Also there is a Jira request on the Shib MDA code to sign a pile of

things and push them into separate files (rather than signing the MDA). Not

difficult.

Use entity categories as filters for MDA. Create the aggregates offline then

sign. Have to know ahead of time what people want to query against. R&S discovery is a reasonable support query as offline signing but not on demand queries as DOS attack (i.e., arbitrary queries -- which can be used as unbounded resource requests).

Next up for conversation:

SOFTWARE requirements for per entity MD requirements.

One Action to add to our list:

AI Ops will communicate about the expired InCommon certs in md in a separate email communication after we communicate about the signing key and CA trust anchor.