SAMLorama Topics and Notes

SAMLorama notes

In the room...

- Nate Klingenstein
- Eve Mahler
- Scott Cantor
- Jeff Hodges
- Drummond Reid (day1 only)
- Andreas Solberg
- Bob Morgan
- Leif Johansson
- Ian Young

Things we haven't covered yet

- The role of DNSSEC
- Fedlet-style bootstrapping

Agenda By Days

Wednesday

XRDS-education / Scaled up discovery

Drummond summarized XRDS. Discussion followed about where to put SAML metadata in all of this. Peter Davies has a document which explains how to reference SAML metadata from XRDS documents. It may be valuable to extract this part into a separate document....

Thursday

Dynamic SAML metadata

Discussion about splitting gruesome gorilla up into metadata content profiles, metadata trust profiles and metadata discovery profiles. SAML profile document may want to include a normative reference to and a requirement for supporting SAML1.x SAML metadata profile for backwards compatibility. This does not mean supporting SAML1.x but rather iff SAMLv1 is supported then you must support SAML1.x profile of SAMLv2 metadata.

Documents names/scope

- Dynamic SAML discovery and trust profile (how you find and place trust in metadata using PKI)
- Minimal SAML metadata profile (how you process metadata and how metadata controls SAML runtime)

Discussion about conventions for metadata discovery mechanism (domain -> metadata). Document (1) should contain a list of suggested methods, eg saml.domain etc. The role of TLS vs document signatures was discussed.

We had a discussion about the nature of key-to-name binding. The consensus was to have a SHOULD for entityID-based binding (cn or subjectAltName) and a MAY for binding to the domainname of the entityID found in the metadata which in itself implies that entitIDs MUST be URLs.

Metadata tagging/attributes/multiple signatures

Ian and Nate describes their usecases which all have to do with annotating metadata in a trusted and distributed way. Concrete usecases are UcTrust in InCommon and London Grid for Learning in UK federation. The problem is how to delegate the validation of the behavioural requirements involved in (say) memberhsip in UcTrust. Ian has another problem: supporting and relaying non-standard extensions that the federation operation doesn't understand. We discussed the semantics of the signature of the metadata. We also talked about the need for naming constraints for extensions and attributes on entities.

There are two basic approaches: a service which associates entities with attributes or a way to annotate entities in metadata.

- Eva M suggested the use of XRDS - define a community/reputation service which could be referenced from an XRDS document which also references SAML metadata.
- Scott explained how Shiboleth allows SAML attributes to be associated with entities in metadata and be exposed as attributes in assertions about users.

Both of these cases could coexist if the service in alt (1) was built using SAML attribute query based on the entityID - i.e a service returning an attribute assertion for the entityID. This could be called both statically by federation operators to aggregate into assertions in metadata or dynamically by SPs.

- Scott to document the Shib behaviour of including attributes in metadata.
- SAML metadata for "entityID attribute query protocol" (which is more or less just a normal SAML attribute query) needs to be written up.

Minimal or subsetted SAML profiles and best practices on SAML 2 usage

Scott: possible starting-point: http://www.cio.gov/eauthentication/technical_architecture.cfm specifically http://www.cio.gov/eauthentication/documents/EAuthFederationArchitectureInterfaceSpec.pdf

We had a discussion about various aspects of the profile. Andreas volunteers to write up a profile reflecting the technical discussion.

Embedded keys vs embedded certs

Friday