LoA technical planning -- DRAFT

Status: planning draft for use by InCommon and NIH dev teams

NIH would like to have qualified InCommon IdPs put assurance labels on SAML assertions sent to the NIH federation gateway, for ultimate consumption by NIH apps that can use identity assurance in their risk processing. InCommon is establishing an assurance program (http://www.incommon.org/assurance/) to qualify IdPs under the InCommon Identity Assurance Framework. This Framework is being reviewed by FICAM for acceptance under its TFPAP. Once all the approvals are worked out and the program is under way, there will need to be technical interoperability to support the program policy goals.

Issues include:

Overall technical approach: We assume it is in everyone's interest to follow the standard described in http://wiki.oasis-open.org/security/SAML2IDAssuranceProfile . This doc, however, specifies a relatively new use of a SAML feature (AuthnContext) that has been little-used, so software support is uncertain, and usage patterns are not well-established. A fallback approach would be to use a SAML attribute to represent the assurance qualifier in the assertion.

- Yes, we'll use the Assurance Profile doc methods. Note that this is SAML2-only.

Will the NIH gateway request LoA? : The SAML assurance profile permits the SP to request a particular LoA (with a choice of matching rules) in the AuthnRequest. This is not required; the IdP can be configured to know that a particular SP needs a particular LoA, and just send it. This however may not meet the NIH use case, because the NIH federation gateway serves many apps, some not requiring any LoA label today, some that will require (or prefer) LoA in the future. With no request, IdPs would have to send the highest LoA on any access, which could be a burden on the user, and could set a bad precedent for LoA pricing in the future. But it could be the easiest deployment for now. The next issue (profile mismatch) applies to requests too.

- Yes, the NIH gateway will request LoAs using AuthnRequest as needed.

Mismatch between FICAM profiles and InCommon profiles: FICAM defines LoAs and identifies them with URIs (example?). InCommon does this also (e.g. http://incommon.org/assurance/silver).&nbsp; FICAM (at some point) will bless InCommon Bronze as comparable to FICAM Level 1, and Silver as comparable to Level 2. The AuthnContext element can contain one (or more?) URI indicating the LoA relevant to the assertion. InCommon IdPs will be certified to issue the Bronze and/or Silver URIs. The NIH SP will presumably normally be looking for the FICAM Level 1 or Level 2 URIs. Either the IdP or SP must deal with the mismatch. InCommon suggests that it is the USG SP that has the policy that Silver is equivalent to Level 2 (e.g.) so the SP should receive the Silver URI and use its policy mapping to accept it.

- The NIH gateway will use the InCommon LoA URIs when making requests of InCommon IdPs, and accept them in responses. Requests will use the "exact match" matching rule, which is supported in the current Shibboleth IdP.
- InCommon should notify FICAM as to the Assurance URIs that InCommon IdPs will send in this process.

ERA or other app requirements? : ERA is talking about being ready to federate by Spring 2012. Probably only some of its functions would require Level 2. Will this mean "step-up" authentication in a single session in some fashion? This will be discussed with ERA, later.

- Discussion with ERA on dates and transition process needs to happen at some point.
- Are there other apps with LoA2 requirements sooner than ERA? Probably, but likely other agencies than NIH. Debbie will investigate and report back.

NIH gateway capability to send AuthnRequest on-demand, and process AuthnContexts? : It is not clear whether the gateway product has support for configurable/dynamic AuthnRequest generation, or handling of non-built-in AuthnContext responses. The vendor will be contacted about this. Testing will happen at some point, probably just intra-NIH, using and NIH test Shib IdP. It may be that a second NIH gateway SP will be needed for Level 2 to make this work.

- Investigation of gateway capability to generate AuthnContext-requesting-LoA needs to happen. The installed CA product (as of 4-Aug-2011) does not appear to do this.

NIH gateway capability to obtain LoA certification info from metadata? : InC will publish Bronze and Silver certification info in its standard metadata. It would be preferable for NIH just to use that, so they'll look into it, but it's not necessary.

- Investigation of gateway LoA-certification-in-metadata capability needs to happen.

Shibboleth IdP capability to respond with correct AuthnContext on-demand, and integration with backing IdMS? : The Shib IdP can support sending different AuthnContexts, and can deal with processing incoming AuthnRequests with the exactmatch rule. How this integrates with the local authentication process, and backend IdMS features, is a local matter, but one where advice will need to be provided. On the InC someone will need to demonstrate the capability and document configuration steps and issues. This can be done with InC-side resources.

- Investigation of Shibboleth 2.x IdP AuthnContext-handling capabilities needs to happen.

NIH review of InCommon 1.1 Assurance docs for compatibility with their notions of Level 1 and Level 2 : NIH will need to review the new InC Assurance docs separately from ICAM, since NIH probably wants to move more quickly, and InC and NIH have had a history of pairwise MoUs. The 1.1 Assurance docs have approved by InC Steering, and are to be submitted to FICAM soon.

- NIH needs to review InCommon 1.1 Assurance docs, or decide to defer to FICAM review.

Use of Bronze/Level 1? : Under the existing MoU between InCommon and NIH, all InCommon IdPs are accepted as Level 1 without needing InCommon Bronze certification. Will this continue to be true indefinitely or will NIH be wanting Bronze certification for Level 1 equivalence at some point?

- Level 1 will continue to be qualifier-free as it is now. LoA will only be required for Level 2 / Silver.

Use of SHA256: FICAM would like its partners to move from SHA1 for signing to SHA256. This includes both signing assertions and signing metadata. (This is unrelated to LoA but is about InC-NIH interop.)

- It may be acceptable to produce a separate InCommon metadata file signed by SHA256. Unfortunately that algorithm isn't supported in OSes known to be in use in InCommon, so moving off of SHA1 will take a couple of years most likely.
- Is signing assertions with SHA256 possible from InCommon IdPs? Yes, but not with a simple configuraton option right now. Even if that were possible, IdPs would have to special-case that option for now, because some SPs won't handle it. In the V3 timeframe, we should have support for the algorithm extension in metadata, so as sites move to V3, we should be able to drive traffic to SHA-256 on a per-SP basis.
- Strategy needs to be nailed down on this issue.