Identity Assurance Qualifiers (was LOA)--A Recommended URI Profile for InCommon

InCommon and NIH have made progress toward federated access to select NIH applications based on university-based identity systems and user attributes. One of the next challenges comes from situations in which a particular institution meets InCommon criteria for stricter profiles of identity assurance in terms of its infrastructure and operations, while particular members of the institutional community may fit stricter or looser profiles in terms of identity proofing and the kinds of identity credentials they use for authentication. This situation will be real for a significant number of institutions.

The question becomes, given a SAML-based approach to Identity Provider/Service Provider (IdP/SP) interactions, how will the profile of identity assurance that applies in a given transaction be communicated from the IdP to the SP. David Wasley, as a member of the InCommon Technical Advisory Committee, has promoted the use of the concept of "identity assurance profiles." This terminology, he argues, will provide a better fit for the situation defined above than the more common term, "level of assurance." The document you are now reading adopts the identity assurance profile model and proposes a way to codify proposed InCommon profiles in SAML assertions.

InCommon has stated that it will define "bronze" and "silver" profiles, and will certify particular IdPs to be in conformance with a named profile provided their operations and infrastructure meet the associated criteria. It is the intention of InCommon that an institution with an identity assurance profile of bronze could reasonably be mapped to what NIST SP 800-63 defines as level of assurance one. Silver is intended to map to NIST level two. The ultimate arbiter is the SP that receives assertions from an IdP. They may well want to do a risk assessment of their applications and then decide which identity assurance profiles are appropriate for each.

The identity assurance of a given interaction of user, IdP and SP is dependent on many factors. However, in the interest of simplicity of operation, it will be desirable in at least some cases for an IdP to assert that a given interaction, taking everything into consideration, fits a particular identity assurance profile. NIH SPs, for example, would like simple assertions of this kind. This essentially means that an IdP would want to make sure that all aspects of a given user's identity proofing, credentials and attribute reliability fit the "bronze" or "silver" profile. Assuming that the authentication technology also fit the profile, the IdP would be warranted in asserting that the whole IdP side of the interaction matched a particular identity assurance profile.

In other cases, it is possible that the SP would like a finer level of detail, with information on multiple aspects of the authentication present in the IdP assertion. Here, too, information on which profile applied would often be of interest to the SP, either as an overall qualification as above or as applied to various elements of the authentication event. The SAML Authentication Context element would be the appropriate means of conveying this information.

We recommend that InCommon assign URIs to the profiles it defines, specifically, that they assign "urn:mace:incommon:iap:bronze" to the bronze identity assurance profile, and "urn:mace:incommon:iap:silver" to the silver profile. MACE-Dir could define an attribute, identityAssuranceQualifier, whose value would be one of the two URIs defined above (or the value"urn:mace:dir:constant:test"). This attribute could be one element of a SAML attribute assertion, and the SP would then have information on the identity assurance of the assertion as a whole.