Assurance Technical Implementation Considerations

DRAFT

Technical implementation of identity assurance requires system changes from InCommon Operations, IdPs, and SPs. This page (and its child pages) capture lessons learned, recommended practices, and outstanding issues regarding the technical aspects of identity assurance.

- SAML V2.0 Support for Assurance
- InCommon Practices
- SP Behavior
- IdP Behavior
- References



The Use of SAML V2.0

Participation in the InCommon Identity Assurance Program requires the use of SAML V2.0 Web Browser SSO. IdP and SP operators should plan to upgrade to SAML V2.0 as soon as possible.

SAML V2.0 Support for Assurance

SAML's support for identity assurance is embodied in a concept called "Authentication Context". The context of an authentication event is designed to capture both technical and procedural elements that factor into the "confidence" expressed by the identity provider in the event. In terms of assurance, this maps to the concepts of technical strength and identity proofing strength that make up an assurance profile.

Every authentication statement issued by an IdP contains an `<saml:AuthnContext>` element that expresses the context of the authentication event. There are a variety of syntaxes supported, but the most common one is to define a "class" of authentication contexts that all share essential characteristics that are of interest to a relying party. These classes are mapped to URI constants that are expressed in an element called `<saml:AuthnContextClassRef>`, of which a single value can be expressed by the IdP in response to an authentication request.

In addition, SAML V2.0 SPs have the capability to include simple or complex matching requirements in their authentication requests that influence the Authentication Context supplied by the IdP. The intent is to allow IdPs that support varying levels of assurance to honor requests based on the requirements of the SP and not a one-size-fits-all policy. In practice, this approach can be tricky to implement and may depend on customization of one's software deployment.

Thus, we expect assurance deployment to be gradual, and we will continue to evolve documentation to reflect what we learn. We also encourage deployers to talk to their software suppliers about the support (or lack thereof) of these features.

InCommon Practices

See: InCommon Practices - Certification and Metadata

SP Behavior

See: Assurance - Service Provider Behavior.

IdP Behavior

See: Assurance - Identity Provider Behavior.

References

- SAML V2.0 Core
- SAML V2.0 Metadata Extension for Entity Attributes
- SAML V2.0 Identity Assurance Profiles

File	Modified
XML File incommon-idp-metadata.xml A complete example of IdP metadata with IAQs included	Oct 10, 2011 by trscavo@internet2.edu