Deployment Profile Working Group Categorized Issues

This page has been deprecated. It was an intermediate work product. The final report and the completed saml2int profile should be used as primary sources of information.

Introduction

This page contains issues discussed by the Deployment Profile Working Group, based on issues remaining in the Deployment Profile - Interop Issues List. The issues are categorized according to the group's assessment of their intended target document.

Index to categories:

For saml2int

Issue(s)	Section	Description
1, 2	5	Published metadata must be signed using a separately distributed certificate.
1, 2	5	Relying parties must consume published metadata on a regular basis because (we are attaching all trust to it). (This needs to move out of "for saml2int", because it presumes that metadata is remotely consumed, which is not currently required in saml2int)
4	8.1	Service providers must be able to initiate an SAML request to an identity provider. Service providers must not require IdP-initiated SSO.
5		Service providers must support deep linking
9, 46	8.1, 9.1	Deployers must support three (3) minutes of clock skew in messages and must synchronize server clocks with an NTP server.
12	5	Deployers SHOULD use long-lived, unexpired, self-signed certificates (published in metadata) for signing and encryption keys, to avoid problems with implementations that generate errors when processing expired certificates. (This is part of MDIOP, so technically shouldn't need to be here, but pragmatically needs to be.)
47	5	Messages and assertions must be signed with a minimum RSA-2048 key length and SHA2 digest.
15	7	Identity providers must be able to release arbitrary user identifiers as attributes in addition to supporting the standard set of NameIDs in the SAML assertion.
15	7	Service providers must be able to accept arbitrary user identifiers sent as attributes in the SAML assertion.
16	7	Service providers must be able to accept one of the standard identifiers sent by an identity provider and map it to an internal user identifier as necessary. Must not require IdPs to support arbitrary attribute names or identifiers.
16	7	Don't try to force a value into a pre-defined format that is not meant to hold it. (do not misuse existing formats)
18	8.2, 9.2	Deployers must be able to extend allowed values of authentication context class to include site-specific values.
17	8.2, 9.2	*Takes precedence over 17a/b, below.* SPs that require specific authncontextclassref values in assertions MUST have an authentication-related business requirement for that restriction. An SP that has a business requirement to limit authncontextclassref values MUST specify the allowable values in the RequestedAuthnContext element of authnrequests it generates. Conversely, if an SP does not specify RequestedAuthnContext values in its authnrequests, *or* if the SP does not support SP-initiated authnrequests, then the SP MUST NOT restrict allowable authcontextclassref values in IdP assertions.

17a	8.2, 9.2	Service providers that do not have a requirement for a specific authentication context MUST NOT specify a requested authncontextclassref in AuthnRequests. Service providers that do not request specific contexts or rely on IdP-initiated SSO MUST accept any authentication context class ref value returned from the identity provider.
17b	8.2, 9.2	Service providers that have specific requirements for authentication context MUST indicate those requirements in requested authncontextclassref in AuthnRequests. Such service providers MUST be prepared to handle any SAML error that might be returned. If a Service Provider requests specific AuthnContextClassRef values, it (or the dependent application) MUST validate that one of the required AuthnContexts was returned in any SAML assertions.
32, 20	5	Deployers must not include endpoints in published metadata that aren't supported.
34	5	Deployers must include a technical contact in published metadata Updated to a contact type that is defined in SAML MD, since security contact type is not. Moving security contact down to 'not for saml2int' - ***Working Group Decision as of 2017-12-21 meeting.***
44	6, 7	Deployers should allow valid characters and value lengths in asserted attribute values.
49	5	Deployers must include a working error URL in published metadata. Relying parties should direct clients to this URL when an authentication error occurs that cannot be resolved locally.
45, 48	7, 9.2	When federating with multiple IdPs, SPs MUST have a mechanism to avoid inappropriate subject ID value collisions across IdPs by either (a) binding values to the asserting IdP such that the same subject ID value asserted by different IdPs refers to a different subject or (b) validating that subject ID values are asserted by an IdP known to be authoritative for that value. SPs and IdPs SHOULD use qualified identifiers in assertions [reference to scope?], with the SP validating the scope of the received IDs against those scopes valid for the asserting IdP. [possible *non-normative* reference to shibmd:scope; non-normative because not all instances will necessarily use or support shibmd:scope]. If qualified subject IDs cannot be used, and if IdPs are not allowed to assert subject IDs that refer to each others' subjects, the SP SHOULD internally store each subject ID associated with [bound to] the asserting IdP. If neither of these approaches is appropriate for a specific use case, the SP and IdPs will need to agree to a custom process to meet this requirement.
1, 2	5	Metadata signatures should be validated upon receipt of new or updated metadata.
10	5, 9.1	MUST support XML Encryption. Requirement for SSO profile: MUST support encrypted assertions. Requirement for SLO profile: MUST support encrypted NameIDs (SLO). All of these need discussion based on whether to require support for XML Encryption as is, with GCM only, or not at all. [revised 11/13, SEC]
28		Deployments MUST rely on SAML metadata conforming to [SAML2Meta] and [SAML2MDIOP] for configuration of trust management, endpoint identification and verification, and signaling of request and assertion signing requirements. Identity Providers MUST rely on SAML metadata conforming to [SAML2MetaAlgSup] in selecting algorithms. Service Providers SHOULD rely on SAML metadata conforming to [SAML2MetaAlgSup] in selecting algorithms. [revised 11/13, SEC]
35		Identity providers must ensure that a request for forced reauthentication results in the client being required to authenticate in a way that proves that the subject is present. [KW - This is worth also adding to an application profile]
27		IdPs must release a persistent identifier to all SPs

13, 14, 43	8 or new section	Service Providers MUST allow clients the option to authenticate specific resource URLs against more than one identity provider. When more than one Identity Provider authenticates the same resource URL, IdP selection SHOULD be supported using the OASIS SSTC SAML v2.0 Identity Provider Discovery Profile.

Maybe for saml2int

Issue(s)	Section	Description
6		Service Providers MUST NOT issue authentication requests inside a frame or via any mechanism that would require the use of third-party cookies by the Identity Provider to establish or recover a session with the user agent. [revised 11/13, SEC]
11		Deployment of new signing and encryption keys MUST be managed [KW: through metadata which is automatically refreshed by peers]. Signing keys MUST be published via metadata for a reasonable period before use, and new decryption keys MUST be deployed in conjunction with existing keys before introduction into metadata (with removal of old keys after a reasonable period). "Reasonable" in this context is subject to the norms of a community. [revised 11/13, SEC][revised 11/17, KW]

Not for saml2int (things we will need to address in our profile)

Issue(s)	Section	Description	Notes
7, 8		Applications that support provisioning of access control MUST allow this provisioning to take place via attribute value mapping for values supplied in the assertion. [SC - this would have to get more concrete if we wanted to require a behavior] [ME - Outside of SAML2int, give guidance to deployers who want to share access control information - example: REDCap] [KW - May be for a class of applications with fully externalized access control]	
39		Deployers should support a non-targeted, non-opaque, persistent, non-reassigned scoped identifier for collaboration across research organizations. (Presume this was referring to IdPs)	
36		Service providers must ensure that a request for forced reauthentication results in a valid current assertion.	
50	7	Deployers should choose from standard LDAP/X.500 (inetOrgPerson?) and eduPerson attributes where possible and should avoid creating custom attributes that duplicate the function of a standard attribute.	
34	5	Deployers must include a security contact in published metadata	

7, 8		Applications that do on-the-fly provisioning: Should use an attribute value to trigger provisioning, and absence of that attribute value should cause deprovisioning	Text from github issue on our saml2int wor, prepared by JudithBush: While most of the discussion about HOW skewed towards an InCommon solution, it seems a brief normative directive addressing the issues below should be included in saml2int. KEY ISSUE: need an attribute that signals provisioning and ALSO deprovisioning an account. Or Don't do online provisioning without an authorizing component. Issue: Deployers should choose from standard LDAP/X.500 (inetOrgPerson?) and eduPerson attributes where possible and should avoid creating custom attributes that duplicate the function of a standard attribute. Define standard so that we avoid, "But this is my standard." Does this imply using eduPerson entitlements instead of group membership? The current tone doesn't seem to imply this, but we think it should. (But that's a preference? And the community wants to go the other way? Or maybe this is rare in Federated exchanges? If the eduPerson schema won't fly in SAML2int, we will add this to the deployment.
NEW		As a deployment, your entityID MUST contain the domain of whatever organization is the owner of the application, in the case of an SP; or the owner of the organization whose users are represented by the IdP, in the case of an IdP.	
NEW		IdPs MUST/SHOULD publish a shibmd:scope in metadata, and asserted attributes MUST(barring something unusual) match the published scope, and SPs SHOULD verify/restrict scopes on asserted attributes to match that scope.	
NEW		Metadata MUST include UI elements for display name. SHOULD include logo, description and privacy policy.	

Not for a profile

Issue (s)	Description	Notes
3, 31	Lack of specificity and sloppy use of SAML constructs	This needs to get converted into identification of an issue for the final report, in the form of testing conformance and InCommon having 'teeth' to enforce. Requirements need to be testable for this to happen.

For federations

Issue(s)	Description
27	Label IdPs that do not release a persistent identifier to all SPs
40	Define a ready to collaborate entity category for IdPs and SPs.
41	Perform regular health checks against all deployers as well as validating all metadata submissions at a per-element level.
34, 39	Label entities which do not meet a specified set of quality requirements.
	Encourage use of per-entity metadata when available and appropriate.
24	Attribute release standards for IdPs
25	Attribute release: suppressing grad students (FERPA concerns)