Deployment Profile - Interop Issues List

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.

This table is a result of copying the original Implementation Profile WG Interop Issues List, and modifying it for use by the deployment profile WG.

Column 1 captures the identified issues.

Column 2 attempts to recast each issue as a "requirement" (note, the recasting may not work, so this column should be looked at skeptically).

Column 3 categorizes the issue per Walter's note.

Column 4 is for record keeping to identify whether/where each issue is captured and addressed in the work put forward by the working group.

Column 5 is a Yes/No indicator of whether the issue is in-scope for the work of the deployment profile WG

This list will also be used ongoing as a "parking lot" for any issues that are raised in discussion that are not immediately captured in the profile documentation.

#	Issue	Issue restated as requirement	Limitation	Resolved	How Resolved	In-Scope for Deployment Profile	Candidate For	Notes	Questions and Answers
1	Manual exchange of metadata or (worse) raw config into	Automated, ongoing metadata exchange and validation	Software /Operational	Yes	Implementation profile IIP-MD04, IIP-ME04	Yes	Saml2int		
2	Security risk /change control risk inherent in one-time MD exchange	Automated, ongoing metadata exchange and validation	Operational	Yes	Implementation profile IIP-ME03, IIP-ME04	Yes	Saml2int		
3	Lack of precise documentation and sloppy use of SAML constructs (in custom deployments)	More specificity for use of some specific SAML features	Software	Yes	Implementation profile - throughout	Yes	Documentation profile		
4	SP-initiated SSO as a "special" case	Support for SP-initiated SSO	Software	Yes	Implementation profile IIP-SSO01	Yes	Saml2int		
5	Lack of deep link support	Support for deep linking	Software /Operational	Yes	Implementation profile IIP-SP13	Yes	Saml2int		
6	Use of frames that break with 3rd party cookies	Keeping authentication screens as top level windows (not iframes)	Operational			Yes	Saml2int		
7	Lack of dynamic provisioning /entitlement-like attribute based authZ	Support for attributes indicating group membership/entitlements (when customers handle authZ)	Software /Operational			Yes	Application profile		
8	Lack of focus on AuthZ space and support	Support for attributes indicating group membership/entitlements (when customers handle authZ)	Operational			Yes	Application profile		

9	Lack of clock skew allowance	Support for clock skew and NTP	Software	Yes	Implementation profile IIP-G01,	Yes	Saml2int	also recommend adding recommendation for consumption of time server service in a deployment profile	
10	Lack of encryption support	Support for XML encryption at the SP	Software	Yes	Implementation profile IIP-SP13, IIP-SSO04, IIP-MD09, IIP-SP02, IIP-MD10, IIP-MD11, Section 2.5 (IIP-ALG01 - 06), IIP-IDP11, IIP-IDP19	Yes	Saml2int		
11	Lack of key rollover support	Support for key rollover	Software	Yes	Implementation profile Section 2.1.3 (IIP-MD07, IIP-MD08, IIP-SP13, IIP-IDP19)	Yes	Saml2int		
12	Requiring valid (vendor signed and /or expiring) certs	Support for long-lived, self-signed certs, which may or may not be expired	Software /Operational	Yes	Implementation profile IIP-MD05, IIP-MD03, IIP-MD11	Yes	Saml2int		
13	Lack of discovery support /portable links (w/o hard coded IdP refs)	Support for discovery services	Software	Yes	Implementation profile IIP-SP09	Yes	Saml2int		
14	Hard coded 1:1 SP:IdP models	Support for multiple IdPs	Software /Operational			Yes	Saml2int		
15	Require non-opaque, non-transient NameID (rather than attribute)	Support for account identifiers in attributes (rather than NameIDs)	Software /Operational	Partial; SP requirements simply state "don't misuse persistent" and "don't require nameid policy in AuthRequests". IdP says "don't require NameID in assertion". Do we need statement about SP accepting assertions not containing NameIDs?	Implementation profile IIP-SP03, IIP-SP08, IIP-IDP12, IIP-SSO05	Yes	Saml2int		
16	Requiring literal account IDs be asserted by IdP	Support for identifier mapping (i.e., IdP ID is mapped to an internal account ID)	Operational	Best Effort: Whether an SP actually supports this is a configuration issue, agreed that the profile allows for the desired configuration, even if a deployment forgoes leveraging the configuration capability.	Implementation profile IIP-SP03	Yes	SAML subject-id profile		
17	AuthnContextClass: not specifying at SP, but failing if PPT not used by IdP	Specify ACC; if unspecified, accept any ACC (unless there is a security reason not to)	Software	Partial; Addresses the requirement in a roundabout way. Does not state "must not require an ACC if it is not specified in metadata". (Not clear that such a requirement would belong in this document, though).	Implementation profile IIP-IDP10	Yes	Saml2int		
18	AuthnContextClass: can't handle locally defined AuthnContextClasses	Allow support of extended ACC's (as part of site-specific configuration)	Software	Possibly; arguably inferable from IIP-IDP10, but it is not clear from IDP10 that IdP must support arbitrary values for ACC.	Implementation profile	Yes	Application profile		

19	AuthnContextClass: no "step-up" support	Support use of "step-up" authentication (re-auth with new ACC and poss ForceAuthn	Software /Operation			~~Yes~~ No (No current accepted practice)	Application profile	App profile at best - Some of these are really hard - probably need to update saml2int and then work backwards from gaps	
20	Assuming Logout URL exists	Verify advertised IdP SLO endpoint before directing user there	Software	Partial; Says IdP must support SLO, but does not indicate that SPs must honor IdP metadata. Do we need an SP requirement here?	Implementation profile Section 4.5 (IIP-IDP17-20)	Yes	Saml2int		
21	Logoff handling	???	SAML	Probably	Implementation profile Section 4.5 (IIP-IDP17-20)	Yes	Saml2int		
22	Expectations of SLO	???	Operational	Partial; (assuming this is largely a duplicate of issue 20)	Implementation profile Section 4.5 (IIP-IDP17-20)	Yes	Saml2int		
23	Browser cookie behavior impacting functionality (sessions not clearing, etc)	???	SAML			No		Probably needs to be called out, somehow, about this behavior	
24	Attribute release standards for IdPs	???	Operational			Yes	InCommon "new rules"	Perhaps attribute release recommendations SHOULD be part of this group's final report	
25	Attribute release: suppressing grad students (FERPA concerns)	???	Operational	Is this and 24 about configuring conditional release of data from specfiic users?	???		Probably needs to be reworded, less specific, ask LIGO folks (Scott K)		
26	Privacy practices: what is actually being kept private?	???	Tangential			No			
27	Standardized and effective workflow for dealing with attribute release	Configuring attribute release based on available context	Operational	Partial; IIP-IDP05 is useful for support of entity categories, and IIP-IDP06 is useful to the extent that including md: RequestedAttributes is part of the operational solution. IIP-MD04 is useful to the extent that consuming or excluding metadata simplifies the process	Implementation profile IIP-IDP05, IIP-IDP06, arguably IIP-MD04	~~Yes~~ No	Application profile	Only addressed in the context of the new SAML subject-id profile	
28	Vendors charging fees for setup and support of SAML	SAML support should be part of base service	Operational			~~Yes~~ No	InCommon "new rules"		
29	Lack of framework /contract terms; change controls, support escalation	???	Operational			~~Yes~~ No	InCommon "new rules"		

30	Lack of testing SP /IdP facilities (test SP, test IdP)	Run a testing SP/IdP for validation purposes during initial integration testing?	Operational			~~Yes~~ No		Recommendation in a final report	
31	Knowledge gaps with some vendors on how SAML works.	???	Operational			No			
32	Advertised but unsupported functionality in metadata (artifact endpoints, etc.)	Advertise only supported endpoints	Operational	Partial; MA01-02 address listed encryption profiles. Arguably the metadata exchange requirements imply some support of this, but no specific requirements are listed.	Implementation profile IIP-MD09; IIP-SP02; IIP-IDP02	Yes	Saml2int		
33	Availability of POP /mechanism for assessing risk	InCommon: stronger focus on POP? [May be addressed in different workgroups]	Operational			No		Deprecated by baseline practices	
34	Publishing metadata contact info for security incident response	Include security incident response (usually security or help desk) in metadata	Operational			Yes	R&E profile	InCommon behavioral/Sirtfi thing	
35	ForceAuthn: IdPs not ensuring user is reauthenticated	Verify function of reauth before resetting authninstant	Operational	Yes; at least to the extent we can define it across authN methods.	Implementation profile IIP-IDP08	Yes	Saml2int		
36	ForceAuthn: SPs not checking authninstant	Verify (or allow verification) of authninstant currency	Software /Operational			~~Yes~~ No (Seen more as advice than profile)	Application profile		
37	OASIS Standards have not been updated with Errata, current Errata out-of-date	Recommend in report-out of WG that someone be resourced to update the Errata and a modify the standard to include the changes from Errata (working with OASIS) (Scott C says someone has informally volunteered to do this. Who?)	Standards	Partial; Addressed separately (Scott C, Eric), but not included in the OASIS repository.	No	Noted		Not part of profile, but may be worth pursuing separately.	
38	Review with REFEDS once a solid draft is done	Nick to check in with Nicole on this	Standards	Nick		Tangential			
39	Research collaboration requirements for adoption of a persistent nameID	Use of persistent nameID or other mechanism to enable seamless collaboration across multiple SPs in a research organization.	Operational	Scott K		Yes	Application profile		
40	"Ready For Collaboration" entity category for IdPs	Description of an entity category that would signal that an IdP is configured for ease of collaboration with no manual intervention by operators, does not re-assign ePPN, and/or uses persistent nameID... etc. TBD	Operational	David W		Yes/Tangential?	Application (or federation) profile		
41	"Red IdPs"	eduGAIN has the "ECCS" service (https://technical.edugain.org/eccs/index.html) for highlighting various levels of IdP operability. Tom Scavo has a script that looks for "dead" IdPs. Is there some useful baseline for IdP operability or interoperability that this group would recommend and could it be tested for?	Operational	Nick / Scott Koranda		Yes	R&E profile	Possibly recommend inserting entity attribute for 'red' IdPs	
42	Don't respond to Unsolicited assertions.	(Still working to clarify specific requirement)	Software			No			

43		Include language in SAML2int regarding support for multiple IdPs asserting against access to the same resource URL/entityID. (I.e., clarify that federation presumes cloud vendors can support multiple IdPs and discovery, not just externalized authentication)	Software /Operational			Yes	Saml2int	Followup to item 14 to be addressed in SAML2INT work	
44	Attribute or NameID values too short or disallow legal XML characters	Minimum implementation requirements for attribute/nameid values (in particular xs:string) length and legal characters	Software	Yes	Implementation profile IIP-G03	Yes	Saml2int		
45	Lack of scope validation	DEDUPLICATE into binding ID to issuer one) Attribute scopes can be validated against allowed scopes defined in metadata (or elsewhere?).	Software.			Yes	Saml2int		
46	Lack of time synchronization (separate from, but as important as clockskew)	Require that SP and IdP deployments use time synchronization against time servers	Operational			Yes	Saml2int		
47	Java and md5/sha1 certificate support	Deployment profile should call out that all certs should be signed with modern signing algorithms to avoid being rejected by cryptographic code that is increasingly aggressive about rejecting older signature types, even in cases where signature verification is not required.	Operational			Yes	Saml2int		
48	Binding of an identifier to its issuer or more broadly checking scope	See:http://www.economyofmechanism.com/office365-authbypass.html	Software /Operational			Yes	Saml2int		
49	Broken or missing errorURL in IdP metadata	Recommend an errorURL in IdP metadata. If an IdP does not have a working errorURL in metadata, it should be tagged with hide-from-discovery.	Operational			Yes			
50	No standard attribute set	Define or reference a standard attribute set. (I.e., do we use eduPerson LDAP objectclass vs. InCommon POP/Wiki vs. some broader spec)	Operational			~~Yes~~ No		Added during 10/6 meeting discussion	

Note: not included here are some recommended reference links, as those have been captured in the working group's list of references already