Interop Issues List

On the initiation of this working group, but prior to the first meeting, Walter sent an email titled "Kicking Things Off" to the group mailing list.

The email asked:

> *1. From both an IdP and SP perspective, what have been the most common challenges you have encountered when attempting to interoperate with federated partners?*
>
> *2. To what extent were the challenges from question one a result of operational practices of the site vs. software configuration vs. limitations in the SAML implementation used?*

This table (you're welcome, Scott!) is an attempt to capture the issues listed in that thread.

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.

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	Relevant Profile Sections	Resolved
1	Manual exchange of metadata or (worse) raw config into	Automated, ongoing metadata exchange and validation	Software /Operational	IIP-MD04, IIP-ME04	**Yes**
2	Security risk /change control risk inherent in one-time MD exchange	Automated, ongoing metadata exchange and validation	Operational	IIP-ME03, IIP-ME04	**Yes**
3	Lack of precise documentation and sloppy use of SAML constructs (in custom deployments)	More specificity for use of some specific SAML features	Software	Throughout	**Yes**
4	SP-initiated SSO as a "special" case	Support for SP-initiated SSO	Software	IIP-SSO01	**Yes**
5	Lack of deep link support	Support for deep linking	Software /Operational	IIP-SP13	**Yes**
6	Use of frames that break with 3rd party cookies	Keeping authentication screens as top level windows (not iframes)	Operational	*Not addressed*	
7	Lack of dynamic provisioning /entitlement-like attribute based authZ	Support for attributes indicating group membership /entitlements (when customers handle authZ)	Software /Operational	*Not addressed*	
8	Lack of focus on AuthZ space and support	As above?	Operational	*Not addressed*	

9	Lack of clock skew allowance	Support for clock skew	Software	IIP-G01, also recommend adding recommendation for consumption of time server service in a deployment profile	**Yes**
10	Lack of encryption support	Support for XML encryption at the SP	Software	IIP-SP13, IIP-SSO04, IIP-MD09, IIP-SP02, IIP-MD10, IIP-MD11, Section 2.5 (IIP-ALG01 - 06), IIP-IDP11, IIP-IDP19	**Yes**
11	Lack of key rollover support	Support for key rollover	Software	Section 2.1.3 (IIP-MD07, IIP-MD08, IIP-SP13, IIP-IDP19)	**Yes**
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	IIP-MD05, IIP-MD03, IIP-MD11	**Yes**
13	Lack of discovery support/portable links (w/o hard coded IdP refs)	Support for discovery services	Software	IIP-SP09	**Yes**
14	Hard coded 1:1 SP:IdP models	Support for multiple IdPs	Software /Operational	*Not addressed*	
15	Require non-opaque, non-transient NameID (rather than attribute)	Support for account identifiers in attributes (rather than NameIDs)	Software /Operational	IIP-SP03, IIP-SP08, IIP-IDP12, IIP-SSO05	**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?
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	IIP-SP03	**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.
17	AuthnContextClass: not specifying at SP, but failing if PPT not used by IdP	Specify ACC; if unspecified, accept any ACC	Software	IIP-IDP10	**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).
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.
19	AuthnContextClass: no "step-up" support	Support use of "step-up" authentication (re-auth with new ACC and poss ForceAuthn	Software /Operation	*Not addressed*	
20	Assuming Logout URL exists	Verify advertised IdP SLO endpoint before directing user there	Software	Section 4.5 (IIP-IDP17-20)	**Partial**; Says IdP must support SLO, but does not indicate that SPs must honor IdP metadata. Do we need an SP requirement here?
21	Logoff handling	???	SAML	Section 4.5 (IIP-IDP17-20)	**Probably**
22	Expectations of SLO	???	Operational	Section 4.5 (IIP-IDP17-20)	**Partial;** (assuming this is largely a duplicate of issue 20)
23	Browser cookie behavior impacting functionality (sessions not clearing, etc)	???	SAML	*Not addressed*	

24	Attribute release standards for IdPs	???	Operational	*Not addressed*	
25	Attribute release: suppressing grad students (FERPA concerns)	???	Operational	*Not addressed*	Is this and 24 about configuring conditional release of data from specfiic users?
26	Privacy practices: what is actually being kept private?	???	Tangential	*Not addressed*	
27	Standardized and effective workflow for dealing with attribute release	???	Operational	IIP-IDP05, IIP-IDP06, arguably IIP-MD04	**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
28	Vendors charging fees for setup and support of SAML	SAML support should be part of base service	Operational	*Out of profile scope*	
29	Lack of framework /contract terms; change controls, support escalation	???	Operational	*Out of profile scope*	
30	Lack of testing SP/IdP facilities (test SP, test IdP)	Run a testing SP/IdP for validation purposes during initial integration testing?	Operational	*Not addressed*	
31	Knowledge gaps with some vendors on how SAML works.	???	Operational	*Out of profile scope* **or** *The entire document*	
32	Advertised but unsupported functionality in metadata (artifact endpoints, etc.)	Advertise only supported endpoints	Operational	IIP-MD09; IIP-SP02; IIP-IDP02	**Partial;** MA01-02 address listed encryption profiles. Arguably the metadata exchange requirements imply some support of this, but no specific requirements are listed.
33	Availability of POP /mechanism for assessing risk	InCommon: stronger focus on POP? [May be addressed in different workgroups]	Operational	*Out of profile scope*	
34	Publishing metadata contact info for security incident response	Include security incident response (usually security or help desk) in metadata	Operational	*Out of profile scope*	
35	ForceAuthn: IdPs not ensuring user is reauthenticated	Verify function of reauth before resetting authninstant	Operational	IIP-IDP08	**Yes**; at least to the extent we can define it across authN methods.
36	ForceAuthn: SPs not checking authninstant	Verify (or allow verification) of authninstant currency	Software /Operational	*Not addressed*	
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	*Out of profile scope*	***Partial;*** *Addressed separately (Scott C, Eric), but not included in the OASIS repository.*
38	Review with REFEDS once a solid draft is done	Nick to check in with Nicole on this	Standards	*Out of profile scope*	Nick

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	*Out of profile scope?*	Scott K
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	*Out of profile scope?*	David W
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	Out of profile scope, in scope for later work of a successor to this group	Nick / Scott Koranda
42	Don't respond to Unsolicited assertions.	(Still working to clarify specific requirement)	Software	*Not addressed*	
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	*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		
45	Lack of scope validation	Attribute scopes can be validated against allowed scopes defined in metadata (or elsewhere?).	Software.		
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	*Not addressed*	
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	*Not addressed*	
48	Binding of an identifier to its issuer or more broadly checking scope	See: http://www.economyofmechanism.com/office365-authbypass.html Issues that need to be remedied in a rev of saml2int: require binding of an asserted identifier to the public key in metadata of its original issuer.	Software /Operational	*Not addressed*	

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