Consultation for SAML V2.0 Interoperability Deployment Profile V2.0

Community Review

This consultation on the SAML V2.0 Interoperability Deployment Profile V2.0 was open from Monday, April 9, 2018 and closed on Monday, May 7, 2018.

Background

While updating SAML2int, the InCommon Deployment Profile working group chose to tackle some of the bigger issues that challenge federations today. To help the reader understand some of the group's decisions, here is a summary of a few of the issues and our rationale behind the requirements for these issues. Feedback on the requirements for these items, as well as on anything else in the document, is of course encouraged.

Identifiers and NameIDs
This section eliminates the use of any NameID format other than transient. In addition, the complex, confusing, and in some cases poorly adopted set of attribute identifiers used today has been replaced with two clear identifiers for communicating the subject. This model leverages the new OASIS identifiers profile: https://wiki.oasis-open.org/security/SAMLSubjectIDAttr. While the identifiers profile is still in draft form, it is stable, and is moving toward final approval. We believe this will make the best practices for identifiers much clearer and the choice of identifiers by service providers more straightforward.

Cryptography
Several major vulnerabilities over the past few years have underscored the importance of modern cryptographic algorithms. Cryptography requirements in this document attempt to set a firm line for what's needed to securely sign and encrypt. At the same time, the working group tried to make the requirements relatively future proof.

Deep linking
This is an issue that can cause significant frustration to those using federated services that lose track of the intended destination during the login process, and the working group saw this as one that needs to be fixed. The requirements for this aren't complex but serve to remind deployers of something that often gets overlooked, especially when federated authentication is tacked on later.

Support for multiple IdPs
This issue works together with deep linking in most cases. Other profiles and earlier versions of SAML2int mention the importance of IdP discovery. This section stresses that any federated application needs to be prepared to work with multiple IdPs, a limitation of many applications today.

Logout recommendations
Federated logout is a long-standing debate in the community. The working group, after much debate, created requirements to establish clear guidance. IdPs need to accept a logout request from an SP and need to publish a logout endpoint. What they do with the logout request is somewhat flexible: there's not a one size fits all. The profile also touches on the danger of an SP performing an automatic federated logout as a result of user inactivity. SP support of single logout requests from IdPs is included, but we chose to leave this optional. We feel that our approach will meet the needs of deployers while leaving room for institutional policy.

Logos
Firm requirements around logos have been needed for a long time. Requirements today even differ from one federation to another -- a problem in the era of eduGAIN. The InCommon baseline expectations provide further necessity for logos. The profile makes some clear guidance for format and size along with suggestions for appearance. The working group tried to be specific while leaving room for artistic interpretation.

Document for review/consultation

- SAML V2.0 Interoperability Deployment Profile V2.0 (Draft)

Document After Consultation:

- SAML V2.0 Interoperability Deployment Profile V2.0 (Draft)

Community Review Agenda/Notes

Number	Current Text	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Action

1	Logo 60 x 80	suggestion: high-res Favicon, Android home screen icons, Apple touch icons and Windows metros icons all use square images to represent websites. As such institutions are more likely to have existing, reasonable looking square logos to represent them. It will make adoption more straightforward if IdP operators can simply upload their schools existing high-res favicon/touch icons rather than creating their own, non-square icon. This site has more information on what existing systems are using https://sympli.io/blog/2017/02/15/heres-everything-you-need-to-know-about-favicons-in-2017/ The handful of schools I spot checked either had hi-res favicon or published hi-res Apple touch icons. FWIW, for SPs that also want to make use of social logins Facebook, LinkedIn and Google all use square logos for OAuth clients	Patrick Radtke	Ken Papai Brett Bieber Chris Spadanuda	Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77
2	Re logo transparency	Non-normative text may include a hint about a black or white border around the logo before the transparency if the background is a critical need of the logo.	Via IIW (Judith Bush)	Brett Bieber	Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12,***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77
3	SP certificate requirements	Section SDP-SP42 ***(editor's note: now SDP-SP39)*** says that an SP's metadata must contain certificate(s) that can be used for signing. But section SDP-MD10 ***(editor's note: now SDP-MD08)*** mentions only encryption certificates for SPs. First of all, this a bit confusing: must an SP's metadata contain a certificate suitable for signing or not? Secondly, if, in fact, an SP's metadata must contain a certificate suitable for signing, why?		Scott Cantor, Peter Schober	Addressed via merge: https://github.com/KantaraInitiative/SAMLprofiles/commit/28a1a98a556d57e79da40702d0eb58681f75fd7c See: https://github.com/KantaraInitiative/SAMLprofiles/issues/79
4	Requirement numbering	Just to head off a bunch of comments, the final renumbering of the requirement blocks isn't done yet pending more tweaks to ordering or updates.	Scott Cantor		Agreed that we will attempt to create a requirement numbering format that is consistent with the Implementation Profile, but not one that is "normatively related" to it. Implementation Profile labels are of the form [IIP-Type##] (e.g., [IIP-MD01] is the first Metadata requirement). We agreed to follow this practice, but not to do numbering until the sections are mostly complete/static. Will need to select a prefix for saml2int requirements as well. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/25
5	Reduce scope of document	The SAML-world already has many pages of documents. In order to be effective, the profile should be as concise as possible and contain the essential points needed for interoperation. And not be a wishlist or best-practice document. I propose to remove the entire section on Logo requirements, on MDUI-requirements and the section on deep linking. Not that these are invalid points, they are just not essential and more of a best practice. Whether or not an IdP has a good logo is, to be frank, not one of our top concerns.	Thijs Kinkhorst		Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. The workgroup agrees that the considerations called out in this section are important foundational principles in support of many common higher ed and research use cases. It is important to call out these requirements -- even if they will not be followed – as without them the usability or interoperability of federated apps can be severely impaired. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77 and: https://github.com/KantaraInitiative/SAMLprofiles/issues/106

6	Key hashing algorithm	`[SDP-MD09] "Certificates used MUST NOT be signed with an MD5-based signature algorithm and SHOULD NOT be signed with a SHA1-based signature algorithm."` This is a confusing requirement. X.509 certificates are used as a container for the key, not as a PKI. A few paragraphs above it is stated that the certificate should be self-signed. Talking about these signing algorithms for the key is not necessary and can confuse the deployers. Propose to drop the entire requirement.	Thijs Kinkhorst		Handled as a pull request. Merged on 7/26/2018. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/80
7	Response signing	[SDP-IDP09] requires that response is signed. We are working with signed assertions (not responses) for many years now and I do not recollect this giving rise to any serious interop problem. So I'm not sure that this is an essential property for interoperability.	Thijs Kinkhorst		Decision was to limit options in the profile for the sake of interoperability. Clarification handled as a pull request. Merged on 7/26/2018. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/70
8	Encryption of assertions	SDP-IDP11 requires assertion to be encrypted. Although I understand that there can certainly be benefits, I don't think it's essential for interop to make it a hard requirement. There are in my experiences many cases that work fine and in which encryption is not necessary per se. Propose to make it a "should".	Thijs Kinkhorst		Decision was to clarify but not fundamentally change the requirement. Handled as a pull request. Merged on 7/26/2018. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/82
9	Subject-id	The document obsoletes the NameID and requires the new subject-id attribute. This new identifier is however still very much in its infancy. I believe that an interop profile is not the place to be pushing new things. It should document existing practices and list proven and established technology that is already in wide use. An interop profile should be about "if you follow these requirements, it will work". Any deployer picking up this document now will quickly find out that many federations cannot currently deliver this attribute at all. So the promise of interoperability by following it then quickly fails. The subject-id is a fine idea but not established technology. I propose to remove anything related to the subject-id. It could of course be codified in a version 2.0 when it has been widely adopted.	Thijs Kinkhorst		***No change made*** NameID, when used outside of a transient identifier, is broken at this time. It is true the response which resolves the issues is in its infancy; however there is no other method for interop that avoids the issues with the existing NameID practices. And, while the subject-id attribute is new, no new software deployments are needed to implement the attribute: adopters can configure their IDPs and SPs to use the attribute as soon as they are ready to comply with this profile. We do not believe an interop profile should codify existing practices when those practices have security issues. An interoperability profile is the perfect place to promote solutions to well understood problems. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/83
10	3.1.4. SAML entityIDs	An entityID SHOULD be chosen in a manner that minimizes the likelihood of it changing for political or technical reasons, including for example a change to a different software implementation or hosting provider. This is not in line with current (best?) practice of making the entity ID match the URL where metadata can be retrieved	Niels van Dijk		***No change made*** This is not a current practice or an established best practice. When followed it creates its own problems that need to be resolved. In particular, an entityID should be chosen in a manner that minimizes the likelihood of it changing for political or technical reasons; for example a change to a different software implementation or hosting provider. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/97
11	SDP-SP05 (removed)	The use of "The <samlp:AuthnRequest> message MUST NOT contain a <saml: Subject> element. This is a relatively unused feature that is supported by few IdPs." While the use of saml:Subject is indeed not often used generically, there is a critical use case for this for step-up authentication, as this typically requires the binding of a LOA to a specific user (as expressed in the subject).	Niels van Dijk		Handled as a pull request to remove this requirement. Merged on 7/26/2018. While including a saml:Subject is not a standard method for managing step up authentication, we will refrain from stating a MUST NOT. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/102
12	SDP-MD11 (removed)	Aspect ratios (and optionally a minimum pixel dimension) may be more helpful than rigid pixel dimensions: e.g. square, 4x3, 16x9.	Brett Bieber		Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77

13	SDP-MD11 (removed)	Vector formats, such as SVG should also be recommended.	Brett Bieber		Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77
14	SDP-MD11 (removed)	Unless the background color logos will be presented on can also be specified /recommended, accessibility cannot be guaranteed with any logo, e.g. white on white. I'd recommend including samples of presentation, removing the transparency requirement, or explicitly stating that logos must have sufficient contrast to be displayed over a white background.	Brett Bieber		Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77
15		Is that merely saying "MUST support up to 5 minutes of skew"? If now I'm confused by MUST min 3 and max 5. (What about datetimes that are only 2 min off, then, below the "minimum" value?)	Peter S.		Clock skew clarification rewording. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/76
16	SDP-G02	mdui:Logo has no explicit allowance for data: URIs so the 256 char limit will cause issues there. The minimum RSA key sizes given in bits are probably seen as falling under "otherwise referenced" and allowing for chars > 256?	Peter S.		Due to conflicting recommendations from several respondents, the workgroup decided to make the the logo requirements less specific in several areas, and provided non-normative text that deferred the specifics to the party's community of practice. We have agreed to remove SDP-MD11, remove SDP-MD12, ***(editor's note: SDP-MD11 and SDP-MD12 exist as new requirements)*** replace SDP-MD13 ***(editor's note: now SDP-MD10)*** with non-normative text that advises the party to determine their community's practice. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/77
17	SDP-SP04	FYI, SimpleSAMLphp currently cannot support this requirement in supported releases (and once the software can lots of deployments may need updating)	Peter S.		***No change made*** The document describes intended behavior, so we expect implementations to fix any related bugs if deployers of that software want to be able to meet the requirement in this profile. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/107
18	SDP-SP17 (was SDP-SP20)	Maybe mention shibmd:Scope here or in SDP-MD01 (the latter if an actual requirement to configure authorized scopes from metadata is intended) so deployers don't need to go hunting how to achieve that scalably?	Peter S.		OASIS have now standardized shibmd:Scope within the subject ID specification - https://wiki.oasis-open.org/security/SAMLSubjectIDAttr , also see SDP-IDP14 for IdP requirement See: https://github.com/KantaraInitiative/SAMLprofiles/issues/95
19	SDP-MD04 (was SDP-MD05)	Does running someone else's amended installer or deployment script that creates, say, a correctly configured backchannel, count as "deliberately and intentionally"? Maybe all that should be required is *working* stuff (e.g. reachable ports with correct keys, etc.), not "intentions"? I agree with the intention (ha!) but practically this seems tedious to enforce (having to ask "Do you really want to support X, and why?") – but then I may actually be doing that already as registrar...	Peter S.		Addressed via merge: https://github.com/KantaraInitiative/SAMLprofiles/commit/3a3425bd1127c1f5c39834f7ec852cc18627b381 See: https://github.com/KantaraInitiative/SAMLprofiles/issues/98
20	SDP-IDP15/16 (was SDP-IDP14/15)	Is error handling at SPs really so bad that IdPs now MUST fail instead of returning to the SP just w/o the requested (via Entity Attribute here) attributes? That seems to require new behavioural rules for all IDP implementations in existence (to fail authn if the SP uses a certain entity attribute and the IDP is unwilling/unable to comply), something that may not even be possible with anything other than Shib or SSP.	Peter S.		***No change made*** Yes, SP error handling is *that* bad, and we were unable to identify a third option beyond returning an empty assertion, which itself causes huge problems. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/99

21	SDP-IDP19 (was SDP-IDP18)	That sounds like a "SHOULD NOT release multi-valued attributes (at least not properly multi-valued as SAML intends)". We certainly don't want to encourage people to violate our own specs (eduPerson's affiliation has a MUST requirement for also asserting `member` for certain other affiliation values) or to release multiple values as one concatenated string instead.	Peter S.		Addressed via merge: See: https://github.com/KantaraInitiative/SAMLprofiles/issues/108
22	SDP-IDP33 (was SDP-IDP31)	84% of IDPs and 77% of SPs in eduGAIN don't have `PrivacyPolicyURL`s today. ACOnet is already mandating them for SPs (we're not at 100% either) but we have not done so for IDPs. Is the requirement for `PrivacyPolicyURL` also for IDPs just an overly broad include from the MDUI section? If not how exactly are those URLs envisioned to be used? IDPs can show an SP's `PrivacyPolicyURL` on the consent (or information) screen, sure, but when would anyone need metadata to show the IDP's own policy? (Niels: at the point in the authN flow where this info could be shown, the user is either already in the IdP and hence already subject to the privacy policy, or the user is not, which makes this the wrong IdP for the user anyway)	Peter S.	Niels van Dijk	Handled as a pull request to remove this requirement. Merged on 7/26/2018. See: https://github.com/KantaraInitiative/SAMLprofiles/issues/101
23	SDP-IDP33 (was SDP-IDP31)	errorURL is even less widely deployed today (8% of IDPs in eduGAIN). Worth the trouble?	Peter S.		Addressed with additional SDP-MD12

See Also

- Trust and Identity Consultations Home
- Deployment Profile Working Group Home
- Note announcing the consultation

https://lists.refeds.org/sympa/arc/refeds/2018-04/msg00016.html