Consultation for the Streamlining SP Working Group Final Report

Community Review

This consultation is closed. It was open from Monday, April 30, 2018 to Monday, May 28, 2018

The final report is here http://doi.org/10.26869/TI.98.1

Documents for review/consultation

- Final Report of the Streamlining SP Working Group
- Streamlining SP Onboarding - Criteria Document
- Streamlining SP Onboarding - Questionnaire

For more information about the working group, please see the Streamlining SP Working Group wiki space.

Change Proposals and Feedback - We welcome your feedback/suggestions here

If you have comments that do not lend themselves well to the tabular format below, please create a new Google doc and link to it in the suggestion section below.

Number	Current Text	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Action (please leave this column blank)
1	NA	Who should maintain the SP questionnaire over time, as the federation evolves?	Nick Roy		
2	"Login Experience - Is the login page accessible and easy to find? What's the experience if a user logs in but is not authorized?	I would suggest addressing IdP discovery rather than a 'login page' in this question. Issues around how a user accesses discovery when provided a link into the service, and whether the target of their link is preserved across IdP discovery and login are important.	Nick Roy	Matt Callaway	
3	"Logout Experience - Does your application support a proper logout?"	What is a "proper logout" in a federation context? Checking to see if there is a SLO endpoint available in the user's IdP metadata, and making a SAML logout request? How should logout be handled at the IdP at that point? The updated saml2int tries to address this issue, but it is complex/challenging. https://kantarainitiative.github.io/SAMLprofiles/saml2int.html	Nick Roy		
4	"to head of additional questioning"	"To head off additional questioning"? - Might be best to actually use this to cause additional questioning of the SP by the person doing the onboarding, in any case.	Nick Roy		
5	Appendix C item 2 "The questionnaire would be encouraged for Service Providers to follow as part of joining InCommon."	Who would receive the questionnaire results in this case, and whose responsibility would it be to work with the SP? At what point in the lifecycle of a prospective participant joining would it be appropriate to inject the questionnaire, and who would do that / communicate with any needed third parties (third parties are assumed to be: the prospective SP, IdP operators at the sponsoring organization (if a sponsored partner), InCommon RA staff, InCommon level 2 support staff)	Nick Roy		
6	NA	Should the report include recommendations to InCommon? Examples might include how to operationalize the questionnaire, recommendations on re-organization of web and wiki content to comport with the WG's criteria and questionnaire, and any areas of work the WG identified that may be valuable for a succeeding WG to address, eg, further refinement of the questionnaire and on-boarding process by soliciting feedback from on-boarding SPs.	Tom Barton	Janemarie Duh	
7	NA	Should Baseline Expectations be mentioned early on since that would be a good thing for new folks to hear? Maybe linking to this blog post or one of the wiki pages would help? https://www.internet2.edu/blogs/detail/15334	MC Martinez		
8	Criteria Document – References – "SAML2 Int Spec"	That's a reference to the SubjectID Attributes Profile, not saml2int	Peter S.		
9	Criteria Document	Great work overall on all three documents. Criteria Document could benefit from a short intro explaining what it is and how it should be used, or how it fits into the big picture	Emily Eisbruch		
10	Final Report	Final Report could benefit from an Overview or Exec Summary at top to briefly state the outputs of the working group, before explaining the WG process and the details.	Emily Eisbruch	Janemarie Duh	

11	Questionnaire	Should the Questionnaire be renamed from "Service Provider Onboarding - Questionnaire" to "InCommon Service Provider Onboarding - Questionnaire and Checklist" ? A concern is the people typically don't like questionnaires, they want something that will help them.	Emily Eisbruch	Janemarie Duh - perhaps even Guide or Responsive /Interactive Guide	
12	Criteria	Do the Criteria recognize the reality that a growing number/majority of the commercial SPs are using commercial SAML implementations rather than either of the two recommended SP implementations ? Are the minimum recommendations supported by the SAML SP implementations that we see in use today by a significant number of commercial SPs ?	Steve Carmody		
13	Criteria	How compatible are the recommendations for SPs with the functionality available from commercial IDPs (eg use of identifiers) (eg OKTA, Ellucian) ?	Steve Carmody		
14	Service Provider Questionnaire	Should this use InCommon branding?	Nick Lewis		
15	Service Provider Questionnaire	"InCommon member" should be "InCommon participant"	Nick Lewis	Nick Roy	
16	InCommon Service Provider Onboarding - Final Report	Appendix C: Add an additional option for campuses to engagement with SPs during the procurement process. Not all procurement requires RFPs.	Nick Lewis	Nick Roy	
17	N/A	More supporting documentation on why to do multilateral federation rather than 1-1 mappings would help SPs understand why they might want to join InCommon.	Nick Lewis	Nick Roy Janemarie Duh	
18	N/A	Need recommendation on if using a different endpoint per campus is recommended or not.	Nick Lewis	Nick Roy - ideally we would recommend they **DO NOT** use different ACS endpoints per campus/customer, but it's not a hard requirement necessarily.	
19	N/A	Should SAML assertions be encrypted? If so, how should this be managed?	Nick Lewis	Nick Roy - YES, given recent SAML /XML vulnerabilities, **assertions MUST be encrypted**	
20	N/A	SAML authN requests should never be required to be encrypted at a message level, as that violates the SAML 2 web browser SSO profile	Nick Roy (added because people get confused by the requirement for encrypted assertions in 20, but there is an antipattern that people fall into where they think that authN requests must be encrypted, when this breaks interoperability)	Janemarie Duh	
21	N/A	How should SPs test their environment in federation?	Nick Lewis	Nick Roy (TBD, we (ops and TAC) are working on a 'test federation' set of requirements now)	
22	N/A	Question about if accounts/access should be provisioned in advance or as access is needed? SPs would like additional guidance.	Nick Lewis	Nick Roy	
23	N/A	Question about how to do de-provisioning? SPs would like additional guidance.	Nick Lewis	Nick Roy (might also be nice to try to get SPs to support SCIM for this to align with TIER/industry, but not a hard requirement)	
24	N/A	Add to the User Experience Checklist: "If your application will be authenticating users via more than one Identity Provider, does your application allow a user to login to the same account from multiple Identity Providers?"	Matt Callaway	Nick Roy	
25	"If your application will be authenticating users via more than one Identity Provider, please be sure to follow the InCommon recommended practices for deploying the InCommon Discovery Service: https://www.incommon.org/federation/discovery.html"	There is no SLA for the InCommon Discovery Service and so the Questionnaire should not imply that an SP must use it. My suggestion is to instead link to the REFEDs discovery guide at https://discovery.refeds.org/.	Scott Koranda		
26	Final Report - Introduction, Appendix A.a., Appendix B. & C.; Questionnaire	Replace references from InCommon member/membership to Participant/participation.	Janemarie Duh		
27	Questionnaire	The Establishing trust section asks for a description of how an SP will distribute and keep metadata up to date if they do not register with InCommon. But it doesn't explicitly call out that changes need to be distributed to IdPs.	Janemarie Duh		

See Also

- Trust and Identity Consultations Home
- InCommon Working Groups Home