Baseline Expectations for Trust in Federation

This consultation on **Baseline Practices for Trust in Federation** is now closed. It was open from **July 6, 2016 until August 10, 2016**

Thank you to all who provided feedback.

Version approved by the InCommon Assurance Advisory Committee, is here:

Baseline Expectations, September 30, 2016

Updated as of February 2018: http://doi.org/10.26869/TI.34.2

Below is the initial draft version of Baseline Expectations, now outdated.

Introduction

As the strategic value of Research and Education Trust Federations ever increases, from time to time it is important to reflect on, then assess and distill what forms the basis for sufficient trust by all participants. On that foundation we can understand gaps and agree to changes that may need to be implemented by various Federation actors in order to sustain trust in them.

What trust do we need to have in Federation? When we rely on Federation, we are partnering with other organizations to do something for us that we would otherwise do for ourselves or forgo altogether. And mostly the latter: Federation makes possible the integration of resources, services, and users across the globe into the myriad ways that the R&E mission is undertaken.

What are the most important expectations of how those partners behave? Is it important to know, fairly promptly, when any of those expectations no longer hold, or is it enough to know that the process by which partners become active in Federation ensures that those expectations are valid?

Below are three short lists of high-level expectations, one for each of three types of Federation actor: an Identity Provider, a Service Provider, and a Federation Operator. What is the gap between these and your expectations of each of them? How would you reframe these so they better express your expectations? Are there any more-detailed needs that must be in this picture, perhaps to be explicitly subsumed within one of the statements below?

Since different specific situations may have higher or lower risk and hence greater or lesser expectations, for this purpose let's focus on establishing the baseline expectations that should be true of all, or almost all, transactions with Federation partners.

Baseline Expectations of Identity Providers

1. The IdP is trustworthy enough to access the institution's own enterprise systems
2. The IdP is operated with institutional-level authority
3. The IdP is treated as an enterprise system by institution-level security operations
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

Baseline Expectations of Service Providers

1. Controls are in place to reasonably secure information and maintain user privacy
2. Information received from IdPs is stored only when necessary for SP's purpose
3. Security incident response plan covers SP operations
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL
5. Attributes required to obtain service are appropriate and published

Baseline Expectations of Federation Operators

1. Focus on trustworthiness of their Federation as a primary objective
2. Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions
3. Internationally-agreed frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted
4. Work with other Federation Operators to help ensure that each Federation's operational practices suitably promotes the realization of baseline expectations, as above, by all actors in all Federations

END OF INITIAL DRAFT

Change Proposals and Feedback -

Number	Current Text	Feedback / Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Resolution
1	IdP expectations	I'd swap expectation 1 and 2	Thomas Lenggenhager, SWITCH	Scott Cantor, Ohio State Maarten Kremers, SURFnet	Accepted
2	IdP expectations	Add something like: The IdP only asserts faculty, staff and student affiliations backed by proper on- and off-boarding processes	Thomas Lenggenhager, SWITCH	Mikael Linden, CSC E Yurick, Gettysburg	Implied by the higher level statement "The IdP is trusted enough to be used to access the organization's own systems"
3	IdP expectations #1	The approach may work for staff, faculty and students but my experience is that even trustworthy IdPs have also users (industry partiers, library walk-in, ...) whose accounts are less secure and wouldn't have access to the key enterprise systems. To make #1 useful for SPs, maybe introduce a tag for the trustworthy accounts (to enable SP side filtering) or make it explicit that #1 applies only to accounts with eP(S)A=staff, faculty or student (c.f. the comment above from Thomas).	Mikael Linden, CSC (NH comment: note it only says that the IdP must be trusted to access enterprise systems, not that all accounts will be authorised to do so).	Maarten Kremers, SURFnet	Implied by the higher level statement "The IdP is trusted enough to be used to access the organization's own systems". Assurance profiles may build on that baseline as may be desired.
4	IdP expectations	The word "institution" should be replaced by the word "organization" to be inclusive of organizations that operate IdPs and that are not institutions, such as LIGO.	Scott Koranda, LIGO	Nicole Harris, GÉANT Von Welch, IU	Accepted.
5	SP expectations	The 5th bullet on attribute requirements is probably a bit over-specified for contractually negotiated situations where specific data exchanged will depend on the customer and the particular relationship, and isn't usable ad hoc. Maybe wording allowing for "or as negotiated by contract".	Scott Cantor, Ohio State	Janemarie Duh, LC	Accepted. New wording: " Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly"
6	FedOp expectations	I would add: "The federation operator makes the trustworthiness transparent to the participants."	Scott Koranda, LIGO		Accepted.
7	IdP expectations	The current POP (2008) states an expectation that IdPs will "provide authoritative and accurate attribute assertions to other Participants" but I don't see that covered in the text above.	Jim Basney, NCSA/Illinois	Janemarie Duh, LC	Noted for consideration in materials that elaborate on what the high level statement "The IdP is trusted enough to be used to access the organization's own systems" may mean.

8	IdP expectations	The current POP (2008) states, "Sending passwords in 'clear text' is a significant risk, and all InCommon Participants are strongly encouraged to eliminate any such practice." If this is replacing the POP, are we losing an expectation about IdPs not using clear text passwords?	Jim Basney, NCSA/Illinois	Mary Dunker, Virginia Tech	Noted for consideration in materials that elaborate on what the high level statement "The IdP is trusted enough to be used to access the organization's own systems" may mean.
9	SP Expectations	The current POP (2008) states, "InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission of the identity information providing Participant." Are we losing the expectation that data will not be shared with third parties? (For InCommon, I think any SP that has signed the Participation Agreement has agreed to abide by section 9, which imposes this requirement on SPs. However, if this Profile were adopted by other Federations, particularly within the EU, we might want to think about language that would restrict what an SP could do with attributes, and restrict it enough so that EU-based IDPs would be willing to release attributes to non-EU-based SPs making this assertion.)	Mary Dunker, Virginia Tech	Janemarie Duh, LC	Accepted. Revised statement is "Information received from IdPs is not shared with 3rd parties without permission and is stored only when necessary for SP's purpose".
10	IdP expectations	"The IdP is trustworthy enough to access the institution's own enterprise systems". I'd make this mor affirmative and lose the "enough". "The IdP IS trusted to access the institution's own enterprise systems".	Nicole Harris, GÉANT	Eric Goodman, UCOP Janemarie Duh, LC	Partially accepted. This informed the new wording "The IdP is trusted enough to be used to access the organization's own systems" but we did not wish to imply that organizations that operate an IdP only for external use cannot meet baseline expectations.
11	IdP expectations / SP expectations	The wording around the security part in the IdP section and the SP section are very different - the IdP only has to "treated as an enterprise system by institution-level security operations" but the SP has the specific expectation of an incident response plan. Better align these.	Nicole Harris, GÉANT	Von Welch, IU Eric Goodman, UCOP	Accepted. Aligned phrase is "Generally-accepted security practices are applied to the (IdP or SP)"
12	SP expectations	Attributes required to obtain service are appropriate and published - does this need a qualified "in metadata" after the published? Do we need a supporting 5 in the IdP section around IdPs publishing tags for support attribute release approaches? (I like balance, it's an OCD thing).	Nicole Harris, GÉANT		Revised language to avoid question of whether it must be published in metadata. Any means of making them publicly known will suffice: "Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly"

13	IdP expectations & general enforcement strategy	I appreciate the careful craftsmanship of the requirements. Here is a general question by way of example related to certain types of IdPs. InCommon has guest IdPs and also test IdPs in metadata. Should we assume that we want to continue to support these types of IdPs for the community? A section on compliance and enforcement would be helpful. For instance, if one of these special IdPs does not conform to one of the four baseline criteria, will the federation operator tag it with a "hide from discovery" tag or remove the IdP from the metadata aggregate? Once we wade into per-entity metadata, what will the enforce technique look like? Publish with/out a tag or not at all? The federation community has been discussing whether the Federation Operator shold be more prescriptive and act with a more direct enforcement practice. Should this be documented here, or in a companion document (e.g., the FOP)? Will each FedOp have a different enforcement practice or a common expectation on behavior? If different, the FOP would be the best location for practice. If commonality is desired, perhaps this document should contain the enforcement practice. (Added at Ann's request.)	John Krienke, InCommon /Internet2		1. All entities operating in the federation must meet baseline. 2. Operational practices will be addressed separately.
14	Claim & Frequency	Should we assume this claim is self-asserted by the entity operator? Being explicit about this would be helpful. How often should baseline expectations be asserted—annually? What happens if an entity operator forgets to reassert (another enforcement question)? There were decisions made in the Assurance program's documentation that could be helpful to contemplate.	John Krienke		Operational practices will be addressed separately.
15	IdP Expectation	Each account is controlled/owned by a single person, who is responsible for its use.	Steven Carmody, Brown	Janemarie Duh, LC	Noted for consideration in materials that elaborate on what the high level statement "The IdP is trusted enough to be used to access the organization's own systems" may mean.
16	IdP expectations #3	If security operations are responsible for operational security justification of a service or not is different in diffferent organizations and countries. It mabe IT operations that has the security justification, not the security operations. Security operations may be only review the operations of the Identity Provider. Suggest a change of wordning.	Pål Axelsson, SWAMID.		Accepted. Informed the new wording: " Generally-accepted security practices are applied to the (IdP or SP)"
17	IdP Expectations	Alternative to Scott K's comment above (#4): State this as "Participant", and reference the InCommon FedOps Policies and Procedures definition of Participant. (I recognize that doesn't work for other federations, but if there is equivalent generic language for "members" at the REFEDS level that would work as well.)	Eric Goodman, University of California, Office of the President (UCOP)		#4 above was addressed without recourse to InCommon-specific terminology.
18	SP Expectations	#7 above states "IdPs will provide authoritative and accurate attribute assertions to other Participants". I think there may be a matching SP requirement (but maybe its just Recommended Practice). An SP should NOT use a successful authentication for authorization purposes; authorization should be based on the attributes asserted by the IDP.	Steve Carmody, Brown		While authN ! = authZ is good practice, its bearing on trustworthiness of the federation is much weaker than the other Baseline Expectations.
19	IDP Expectations	While no identity proofing requirements are specified, it is expected that organizations operating IdPs will use reasonable care when issuing Credentials to confirm that a single individual applies for and receives a given Credential and its Authentication Secret.	Steve Carmody, Brown		Cf. #15 above.

See also:

Consultations Home

InCommon Assurance Home

InCommon Assurance Call of Nov 2015 on Baseline Practices

- No