Baseline Expectations for Trust in Federation

Last Call for Comments

InCommon Assurance Advisory Committee

Chris Spadanuda, Chair

Associate Director, Core Enterprise Services,
University of Wisconsin-Milwaukee

Introduction

- InCommon, together with R&E Federations internationally, is the foundation on which a global access management infrastructure is being built for the R&E sector
- The InCommon Assurance Advisory Committee (AAC) has developed short, simple, high level statements of how Federation are IdPs, SPs, and Federation Operators should behave to merit our trust in them, and hence trust in the federation they comprise
- Here they are, and we'd like your feedback
- "Consultation" page for gathering feedback (July 6 - Aug. 10, 2016) https://spaces.internet2.edu/x/qYLmBQ

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

Feedback to date on the Consultations Page

- 9 Identity Provider Suggestions
- 4 Service Provider Suggestions
- 1 Federation Operator Suggestion

Suggestion #1

IdP expectations

I'd swap expectation 1 and 2

Suggestion #2

IdP expectations

Add something like: The IdP only asserts faculty, staff and student affiliations backed by proper on- and off-boarding processes

Suggestion #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

Suggestion #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.

Suggestion #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"

Suggestion #6

FedOp expectations

I would add: "The federation operator makes the trustworthiness transparent to the participants."

Suggestion #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

Suggestion #8

SP 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?

Suggestion #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?

Suggestion #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".

Suggestion #11

IdP and SP expectations

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

Suggestion #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).

Suggestion #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.

Suggestion #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.

Suggestion #15

Trustmarks

This approach is a huge improvement over the current, rather outdated, approach of asking sites to publish a POP containing text.

However, this profile contains the word BASELINE in its title; I'm also struck that it doesn't include mention of some items that were supposed to be included in a POP statement. The obvious examples are already called out in the feedback (eg #7, 8,9).

Once this Baseline profile is promulgated, is the AAC planning to develop additional profiles layered on top of the Baseline? Trustmarks of some sort ? Should the community push to raise the proposed Baseline at least to the level of the POP, or even to a "reasonable level for today's world" ? Or should we wait for the follow on set of profiles ? If this is the case, has the AAC begun to think about what that set of profiles might be?

I was wondering, in particular, whether we'd expect to see a profile targeted at IDM Management Policy and Practices. Jim Basney has already called out one such item ("IdPs will provide authoritative and accurate attribute assertions to other Participants" - I read that to mean that the site de-provisions properly when someone leaves; it also means that the site maintains Affiliation values, etc as a person's role changes). Another example might be "each account is controlled/owned by a single person, who is responsible for its use”. I expect all sites to behave consistent with those practices. I'm asking if AAC sees those as Baseline practices, or as items in a layered profile related to IDM practice?

Last Call

- Discussion
- Submit your feedback by Aug. 10, 2016
- https://spaces.internet2.edu/display/InCAssurance/Baseline+Expectations+for+Trust+in+Federation