Assurance Call of 6-July-2016-Comments in AdobeConnect Chat

This page is to preserve the comments in the chat during the Assurance call of July 6, 2016 on **Baseline Expectations for Trust in Federation.** For the full webinar and the slides, see **here**

Emily Eisbruch: Welcome

Dean Woodbeck, InCommon/Internet2: You can download today's slides from the assurance wiki: https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Assurance+Program

Emily Eisbruch: Wiki page for feedback on Baseline Expectations
https://spaces.at.internet2.edu/display/InCAssurance/Baseline+Expectations+for+Trust+in+Federation

Scott Cantor: MDUI probably should be defined somewhere for the less wonky among us.

David Bantz, U Alaska: "enterprisei systems" begs for ellucidation

Benn, SCG: How do you define "enterprise"? eg If a university has an IdP, but so does a school within the University?

Scott Koranda: Institution should be replaced by organization to be inclusive of organizations that are not campuses.

Benn, SCG: sorry meant "institution" not "enterprise"

Chris Spadanuda, UW-Milwaukee: Thank you for the feedback, Scott K. How do you feel about the word enterprise? Is there a better choice of words?

Scott Koranda: There is a better choice of words and I am confident others are going to "beat you up" to find it.

Nick Roy (Internet2/InCommon): +1

jack suess: I think it is enlightening to have the POP highlight what systems are accessible by the IDP on campus?

Scott Koranda: The POP is not a useful vehicle Jack becuase InCommon does not enforce making them available for inspection by all participants.

Paul Caskey - Internet2: @Scott, that's one reason among many. They are not comparable, no standard format, not machine readable, not maintained, etc.

jack suess: I think in #1, there are degrees of trustworthy

Eric Goodman: Is there some formal industry term that can be referred to rather than "enterprise"? E.g., sufficient for accessing sensitive PII data/FERPA/HIPAA (not sure any of those are universal enough to work)

Paul Caskey - Internet2: @Jack, but this is designed to be a "baseline", so no levels in that context

Tommy - SMU: who asserts the trust worthiness of the IdP on the home campus, and what is divulged about vulnerabilities in that assertion?

Paul Caskey - Internet2: @Tommy, there's been debate about whether the exec or site admin (or other) would do that. Not sure I understand the 'divulged' question. The idea is that there would be 100% agreement on the statements (binary agree/disagree).

Chris Spadanuda, UW-Milwaukee: @Tommy - We have been discussing who asserts and recevied feedback at the Global Summit that it should be the InCommon Executive, Others have said it should be the site admin

jack suess: Is #5 reasonable for most providers, often this is contractually defined

Chris Spadanuda, UW-Milwaukee: We are looking for addational feedback on who asserts

Paul Caskey - Internet2: @Jack - this helps automate attribute release...

Dedra - Cirrus Identity: I do think some mention of policy compliance would be good. To indicate that policy compliance aorund attributes that are released and how they are handled must be negotiated with the organization directly

David Bantz, U Alaska: Is there a responsibility to respond to issues arising from non-comforming technical behavior? I'm thinking of "requiring" a format of "unspecified" or relying on "friendlyNames" rather than Names?

Tommy - SMU: @Paul, regarding my comment on potential for divulging too much information, if my IdP is not trusted internally, I'm just wondering whether making that fact known indicates there is a problem with my IdP that could make it a target?

Paul Caskey - Internet2: @David - that would be more of a deployment profile, which another group has contemplated developing

Paul Caskey - Internet2: @Tommy, failure to agree to that would warrant sanctions, which have not yet been detailed

jack suess: I would of expected that the federarion would be audited

Nick Roy (Internet2/InCommon): @David, if you are interested in the deployment profile work, send a note to Walter Hoehn, chair of that WG (wassa@memphis.edu)

Scott Koranda: I have the expectation that the federation operator makes the trustworthiness transparent to the participants. Should that be articulated?

Paul Caskey - Internet2: @Scott - good suggestion - please add a row on the wiki feedback page

Tommy - SMU: @Paul - understood, i'm just grappling with the idea of an IdP not being trusted internally which seems very odd indeed.

Scott Koranda: Bad, bad connection here. Missing some audio. Sorry.

Dedra - Cirrus Identity: Perhaps #3 should include some mention of promoting federation interoperability in general, not just related to improving trustworthiness.

Warren Anderson (LIGO): @Tommy - I can imagine a scenario where I use a simpler authentication method internally (say Kerberos) but stand up an IdP to allow my users to access external SPs.

Nick Roy (Internet2/InCommon): @Tommy @Warren, that is exactly right. Some IdPs are not operated as a 'first-class citizen' when it comes to internal security practices.

Nick Roy (Internet2/InCommon): *Or, _could_ be operated

Eric Goodman: Just the vagueness of the terms discussed above.

Eric Goodman: "enterprise" mostly.

Eric Goodman: We've had audits fail in the past due to requirements not being clear enough to audit against.

Eric Goodman: (I know that auditing isn't necessarily a formal requirement here)

Nick Roy (Internet2/InCommon): From my perspecitve, auditing of this stuff is going to be an anti-pattern if we need everyone to agree to this baseline.

jack suess: For baseline requirements these are fine. We are in compliance.

David Bantz, U Alaska: It can be useful internal guide to ask yourself what would constitute auditable compliance

Chris Spadanuda, UW-Milwaukee: Would it be better to swap out the word enterprise or define it in an appendix?

David Bantz, U Alaska: depends on who has to "sign off" on baseline compliance; if operator, OK; if CEO with legal counsel, would be difficult

Warren Anderson (LIGO): I think reassignment is above baseline, but an interesting addition.

Eric Goodman: @Chris: Probably, but I don't know what that word is.

Scott Cantor: @David, we provided that same feedback during in-person review

Scott Koranda: Self-attestation is enough to get a baseline for InCommon, which really has no useful baseline now.

Chris Spadanuda, UW-Milwaukee: @Eric Thank you. We have time to think of the right wording. Please feel free to add suggestions to the wiki space

Tommy - SMU: It seems any organization serious about federation would be able to agreee with these.

David Bantz, U Alaska: I think POP backs attestation by asking for description of processes; not a bad model!

Tommy - SMU: Maybe there are all kinds of problems with this, but would it help to make certain parts of the attribute filter visible to the federation operators? Just as a method of demonstrating the trustworthiness of the IdP.

Nick Roy (Internet2/InCommon): Not sure I see how publishing the attribute filter makes things more transparently trustworthy

Nick Roy (Internet2/InCommon): It might demonstrate how interoperable or not the IdP is, but that's about it

jack suess: Here is the NSTIC IDEF requirements for the SALS --https://wiki.idesg.org/wiki/index.php?title=Baseline_Functional_Requirements_v1.0

Scott Koranda: @Jack I would phrase it like this: it is hard to explain to the CSO of a large national research project why and how they should trust the InCommon trust fabric.

Scott Koranda: What should we expect next for this process and timelines?

Paul Caskey - Internet2: @Scott - more mature and advanced discussions at TechEx?

Paul Caskey - Internet2: @Scott - with hopefully a detailed implementation proposal

Scott Koranda: A good start as a baseline, yes.

Warren Anderson (LIGO): Not with out CSO.

Emily Eisbruch: please add your feedback here: https://spaces.at.internet2.edu/display/InCAssurance/Baseline+Expectations+for+Trust+in+Federation

Eric Goodman: Thanks!

Scott Koranda: Thanks.

scott (UCLA): Thank you.

Chris Spadanuda: Thank you!