2019-Dec-11 at TechEx in New Orleans

CTAB Open Meeting at 2019 TechEx, Dec 11, 2019

https://meetings.internet2.edu/2019-technology-exchange/detail/10005609/

Thanks to John Krienke for these notes

For reference

- slides from Dec 10, 2019 session: InCommon Updates: Baseline Expectations, Managing Metadata, and More
- https://meetings.internet2.edu/media/medialibrary/2019/12/10/20191210-wu-incommon-update-v2.pdf

Discussion

Welcome and Intro

- Introduction of CTAB members and new incoming CTAB members. Names are on the InCommon website here.
- CTAB wiki is here (FYI).
- Thanks to the community for support in the efforts to increase trustworthiness of Federation.
- Much was accomplished in Baseline Expectations Phase 1.
    - See blog https://www.internet2.edu/blogs/detail/17232

Baseline Expectations (BE) next phase

Review 5 items for proposed community consensus:

- TLS 1.2

- SIRTFI (more info here)
- Error URL
- R&S
- REFEDS MFA

What issues do you anticipate we'll encounter with each of these?

What timeframe should we ask the community to meet each of these requirements?

A rough timeline framework for BE next steps:

- Begin Community Consensus process in Q1 2020
    - This will be our first official use of the Community Consensus process.
- Assess timeline from the community to meet the specific
- Finalize recommendations in a community consensus process

All these steps may take up to one year from concept presentation, consensus process, implementation, and may vary based on community uptake.

Additional topics and notes:

Community Dispute Resolution Process. To remedy disputes between and among InCommon Participants.

Important to note: There is no unilateral decision that CTAB will make to change Baseline Expectations. The community consensus process is always invoked for changes.

A Guidance Document is being created by Albert Wu of CTAB. (v1 adherence draft, clarifications on new items)

Discussion of the 5 proposed changes:

SIRTFI: SIRTFI is also making some changes. How will the changes and requirements be managed? SIRTFI will manage versions with version control numbers (i.e., 1.0, 2.0).

- Does Sirtfi risk lawyers being involved?
- Attesting to compliance might present a legal risk to the organization
- CTAB and SIRTFI members are discussing ways to field test compliance and report back to the GEANT task force. There is also a peer review process in the HPC community, involving a questionnaire, feedback, discovery, remediation, etc.

TLS: Moving targets may also be an issue with TLS as well. There might be a way to use a benchmarking tool like SSL Labs.

- Dependency noted that we would be dependent on how SSL Labs updates its own rankings/grades
- SUNet, Only allow B or greater, only allow a slack time of a week.

- Need to figure out how to make people aware of impending SSLLabs changes
- TLS is a technology. SIRTFI is a set of practices and policies. Are there differences to be aware of?
- Nick - Can we require TLS for endpoints and then drop the attribute encryption requirement for SP endpoints that is often a problem for SPs?
- Active scanning of endpoints. Nick. We updated the InCommon participation agreement when Baseline Expectations were added. There is latitude now that would/could include permission for InCommon to actively scan endpoints in published metadata.
- TLS: if we get too restrictive, we will start having to drop support for certain browsers. This could also be very problematic for hospitals who must run old versions of browsers in patient-facing services.
- Can we have a report-back interface that summarizes browser versions in the TAP versions and instructions for non-TAP?

Ways to measure each of the components of BE. The guidance document (URL above) intends to capture how we will implement and measure meeting each requirement.

ErrorURL: This one speaks to a consistent user experience. What content should be on the page? Comments?

- General advice. What is the error related to? Missing attributes, MFA, etc?
- Sweden: send back a cropped URL related to the issue.
- Basically all errors that SP's can't do anything about
- SAML2Int mentions requirements for this as well
- Perhaps also include a few standard SP-related problems that IdP support can forward to the SP operator.
- Let's get a working group of some kind together to develop a standard around this (a possible Advance CAMP topic for later in the week)
- SP error Guidance. Do we take this up, or just mandate IdP ErrorURL?
- Proxies! (how will they handle specific error URLs?)
- Error URL is *only* about critical problems where the user cannot proceed. Agreed?
- We can get better incrementally. We don't have to mandate a perfect, all encompassing solution.
- Logos for both IdP and SP could also be included in the guidance for good error reporting behavior.
- There was agreement that ErrorURL is for sending users to on a fatal error where the SP can't function. Otherwise the SP should continue, perhaps suggesting the user contact the IdPO about the "problem".
    - For reference, Here are notes from the Dec. 12, 2019 ACAMP session on Error URL: https://docs.google.com/document/d/1SBQtxlkUxgiOPcS6XanhzmOrB-l0y1gsKFhJIyqtBFo/edit

MFA: Just the ability to signal MFA.

- Are we excluding any commercial vendors? An important consideration.
- Can ADFS do this? Does all IdP software support this capability?
- Some other component (bridge, hub, proxy, IdPaaS) could provide this capability.

Begin communicating now that changes are afoot, even though we may not be ready with the actual recommendation.

Maybe a Roadmap that we will eventually be going here.

SP side. We need to tap into new voices.

End of session.