2020-May-5 BE v2 Office Hours

Background for this Office Hours call:

- https://incommon.org/news/open-discussion-slated-for-new-baseline-expectations/

Attending

CTAB Members on this call

- David Bantz, University of Alaska, CTAB Chair
- Rachana Ananthakrishnan, Globus, University of Chicago
- Pål Axelsson, SUNET
- Tom Barton, U Chicago, Internet2
- Brett Bieber, University of Nebraska
- Richard Frovarp, North Dakota State University
- Jon Miner, University of Wisconsin, Madison, CTAB
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Eric Goodman, UCOP - TAC Representative to CTAB

Guests

- Jeffrey Crawford, UCLA
- Mark Boyce, UCOP
- Jason Michelle
- Timothy Johnson, A.T. Still University
- Andrew Morgan, Oregon State University
- Ahsen Baig, College Squares
- Anne Marie Alexander, Emory
- Michael Barrilleaux, LSU Health New Orleans
- Alan Buxey, MyUniDays, Co-Chair of REFEDs Baseline Working Group
- Jordan Dolese
- Jon Sobel, Yale University
- Judith Bush, OCLC, international Library Consortium, Co-Chair of Federation 2.0 Working Group
- Tommy Doan, SMU
- Alan Bowen, Franklin & Marshall College
- Warren Leung, UC Irvine

Internet2

- Kevin Morooney
- Albert Wu
- Ann West
- Nick Lewis
- Jessica Fink
- Emily Eisbruch

Discussion

Welcome and Introductions

Overview of Baseline Expectations (Albert)

- InCommon introduced and implemented Baseline Expectations V1 (BE V1) in 2019
- currently 100% adherence
- https://incommon.org/federation/baseline/
- BE V1 focused on interoperability and contact info

- Now starting consensus for next iteration, which is BE V2.
- BE V2 focuses on security of federation

Three additional statements are being proposed to BE V2:

- All entity (IdP and SP) service endpoints must be secured with current and supported transport layer encryption.
- Entity (IdP and SP) complies with the requirements of the Sirtfi v1.0 trust framework.
- Identity Provider must include an errorURL in its metadata.

See the be2-faq

In addition, two other elements were discussed, but not included in BE V2 due to implementation considerations:

- require support for REFEDS MFA
- require all InCommon IDPs to support R&S

Comments

Andrew Morgan:

- Interested if there will be a requirement to **achieve a certain level of TLS** for all participants
- TLS V 1.2 for example

D Bantz and Brett:

- CTAB talked about requiring a certain grade, doing testing using a tool such as Qualys https://www.qualys.com/
- Interested in feedback on this
- what is required for a grade of A can change from time to time
- so CTAB tried to describe things at a high level
- we need to have reasonable expectations for the community, look at risks

Andrew Morgan: using a tool like Qualys makes sense

Mark Boyce:

- Issue of what browsers are doing around TLS support
- Can't eliminate support for people because of their browsers, but can't leave gaping holes

Judith Bush:

- Several years ago, OCLC found some libraries were working with older browsers and this caused issues.

=======

Jeffrey Crawford:

- question about scope for the BE
- For example, running **IDP Proxy** for health system
- Do we need to check what we are proxying?

Brett:

- Great question, we need to think about this in terms of raising level for our own infrastructure.
- BE helps define relations with entities we are working with
- Create standards for all integrations

Jon Miner:

- InCommon can't mechanically manage testing around proxied entities.
- If issues arose, they could be addressed through the dispute resolution process. https://incommon.org/federation/dispute-resolution/
- The goal is to raise the bar

Mark Boyce:

- if proxying, you can make requirement on back end part of the price of admission.

Other comments

- Wouldn't the statement that "we are secure" apply to end to end transport?
- InCommon will strive to provide guidance behind the baseline expectations

======

Alan Buxey:

- Many installations terminate the TLS on the front end
- the Shibboleth instance is just on HTTP behind the front load balancers.
- Would this affect such architecture?

Albert:

- Reason we ask for SP encryption of endpoints, in SAML assertions, user info is being posted to an SP doing sign in
- In theory SAML has mechanism for encrypting the message
- Problem: a lot of SPs lack the support for the SAML message encryption
- So we want to guard against the transit issue
- Once the message lands at the endpoint we have less concern

Tom Barton:

- We aim to improve trust and interoperability and user experience in the use of federation
- Less concerned about the internals of the IDP and SP
- Concerned about the interfaces, Focus on the federated part of the process

====

Concerns about the SIRTFI self assertion requirement?

- Entity (IdP and SP) complies with the requirements of the Sirtfi v1.0 trust framework.

Andrew Morgan

- Oregon State asserted this, with IAM being the point of contact if there are issues
- Found it to be a low barrier
- Need to update process for a compromised account remediation
    - Do we need to consider what federation SPs they might have accessed.
    - Not too hard, since mandatory MFA is in place

Alan Buxey: suggestion to do **tabletop exercises around SIRTFI**

Brett B:

- Table top exercise is helpful
- Testing the capacity to do tracing, do we have end users IP
- Might be helpful for CTAB to suggest tabletop exercise
- Every institution will need to check the box for SIRTFI, does this mean they have done a table top exercise?
- It's a new world and interacting w federation around security incidents. Understanding the tentacles

Kevin Morooney: supports suggestion for SIRTFI tabletop exercise. Might do a table top exercise it in real time, with a moderator

====

Enhanced Error URL handling

- First phase, having an error URL is a good starting point
- User experience exercise can you give guidance
- Should BEV2 require adherence to the suggestions from the REFEDs Best Practice around Error Handling Working Group?
    - https://wiki.refeds.org/display/GROUPS/Best+Practice+around+Error+Handling
- There is baseline and then there is having a great user experience
- CTAB likely can point to the REFEDs guidelines but won't require that high level

Albert:

- if an IDP can implement what is being recommended by the Best Practice Around Error Handling working group, that is great
- Follow guidance about when an SP should report back to the IDP .
- InCommon can recommended a process even if it's not required by Baseline Expectations

R&S

- Andrew M: Regarding require all InCommon IDPs to support R&S, there is an R&S v2 coming.
- David B: yes this is one reason we are not including R&S in BE2

===

Timeline: for implementing BEv2

Recap of adoption process (Albert)

- See Processes to Maintain Baseline Expectations by InCommon and its Members for details: http://doi.org/10.26869/TI.105.2

- We are now in consensus process period https://incommon.org/federation/community-consensus/
- For review of rough draft: be2-faq
- Then CTAB firms up the statements and will create official proposal for BE v2
- Move to consultation
- Federation adopts BEv2
- Start an adoption period
- BE1 took a year to bring everyone into complete adherence
- BEv2 may take less time, since we have good contact info, due to the efforts under BEV1

- How long should BEv2 consensus process run?
- After BE v2 is final, how long to bring community into adherence
- How long for the implementation?
- Figure out a reasonable timeframe, sample random federation members to ask them about the impact and timeframe

Thank you for joining, your input influences how we move forward.