2021-Aug-3 CTAB Public Minutes - Office Hours Call

Baseline Expectations V2 office hours

Tuesday, August 3, 2021

21 participants

- 11 CTAB and Internet2 staff
- 10 additional community members

From CTAB and Internet2 staff

1. David Bantz, University of Alaska (chair)
2. Ercan Elibol, Florida Polytech Institute
3. Richard Frovarp, North Dakota State
4. Eric Goodman, UCOP - InCommon TAC Representative to CTAB
5. Meshna Koren, Elsevier
6. Jon Miner, University of Wisc - Madison
7. Andy Morgan, Oregon State University
8. Johnny Lasker, Internet2
9. Albert Wu, Internet2
10. Netta Caligari, Internet2
11. Emily Eisbruch, Internet2

Plus an additional ten community members

Reference: Baseline Expectations for Trust in Federation wiki

Discussion

Concern:

- Issue with CTAB showing Qualys SSL Labs scores that are not accurate (too low).
- Our organization verified that our endpoints got A rating in Qualsys SSL scan
- What can we do to make sure that the rating InCommon shows is corrected?

Albert provided background:

- One of ways InCommon measures current and trustworthy encryptions is to run a Qualys SSL tes against connection endpoints in metadata
- Endpoints must be accessible from public Internet in order to be scanned,
- If behind firewalls, we can't scan
- We scan in batches and it takes time
- Your server could be down for maintenance
- if you can scan and get good score, you are OK
- In fall 2021, CTAB hopes to have an improved process around how to handle a situation where InCommon shows wrong or "out of date" SSL score

DavidB

- One community member reported that if you go to Qualys SSL Labs website to scan, you can only scan a 443 port.
- There are other services that will give report back on what TLS encryption you have
- Though it is a less comprehensive report

- Albert provided this link to set of scripts, a set of command line scripts you can run on your own https://testssl.sh

Comment

- We have a Windows Server running Shibboleth connecting to InCommon and have turned it off because of non-use.
- Since the BEv2 deadline, we have not seen any issues.
- We wanted to get this running on ADFS, but cannot seem to get any help in doing so.
- **We really only use InCommon for Certificates.**

Albert

- If you are only using InCommon for Certificate Service, Baseline Expectations does not apply to you.
- So you don't need to register ADFS server in InCommon
- Additional info on ADFS:
    - Potentially helpful resource: https://adfstoolkit.org/content/

    - ADFS out of box does not support some capabilities that federation depends on
    - Does not consume the metadata aggregate in the format we produce.
    - That can be an effort in operations and becomes unsustainable over time.
    - Want to be able to automatically download and consume the metadata.
    - Change endpoints and signing keys.

Comment

- Trouble getting IDP updated. Had old Shib service.
- Now in published state and meeting baseline.
- I guess we are OK.
- Want to use Azure identity services in future as SSO system , thru enterprise applications, not sure if anyone has gone thru that path, of using enterprise applications with InCommon.
- Using a tool called PortalGuard from BIO ID, was Distal Serve https://www.bio-key.com/portalguard/
- Can be set up as a SAML identity provider
- Integrated easily
- To extend integration, would be better to get systems to using the Azure Identity services for single sign on

Comment

- ADFS , with Azure SSO, won't talk directly to InCommon federation.
- Look at a proxy service such as Shibboleth.
- Hoping for more seamless integration

Albert

- When you use SAML, and there is a neutral integration
- If you are using Azure, when they work with Microsoft, go with the Microsoft integration
- When you plug Azure into federation, like ADFS , there will be shortcomings
- Not able to process metadata automatically , won't be able to send certain signals, such as around MFA
- With Azure, you cannot change entity ID
- Microsoft Azure automatically issues an entity ID and you can't change it

Comment

- Cloud protection with Azure Identity protection is nicely integrated
- based on location and travel
- As we have MFA enabled for more users, It helps give us more comfort level on health of environment

Comment

- Single sign on across Calif. community college system
- Looking at OKTA, things in flux
- Looking at common platform
- Many colleges on different systems
- People developing their own solutions. More efficient if we all use the same services
- Interested in success stories with other HE systems
- Suggestion: Reach out to Eric Goodman or Albert

    - UC has its own identity federation
    - That is a subset or superset of InCommon
    - Builds on InCommon standards

Question

- I stopped receiving emails from InCommon about please comply with BEV2. Does that mean I am in compliance?

Answer

- you can **go to federation manager to get a check on that**
- if you are already in compliance you won't get emails
- InCommon temporarily paused the biweekly email notice as we transitioned to BEv2 on July 19.

- At start of July, a good number of institutions asked for an extension of one month.
- The plan is for InCommon to communicate again in the 2nd half of August 2021

General question to attendees:

- What has it been like on your campus implementing BEv2? Anything you'd like to share?

Comments

- Security officers, like IDP operators, tend to be like lawyers or mathematicians at times.
- If they think of a counterexample, they are reluctant to asset SIRTFI
- Took time to get ISO to sign off on SIRTFI
- Problem was with the **acceptable use policies**

- Alumni and parents get logins via the IDP
- Everyone logging into the research sites is covered

Comment

- Security officer was hesitant until we were very careful to scope the requirement to apply to incidents among InCommon federation participants.
    - Did not want to be committed to using those exact procedures in all other cases.

Comment

- Took several rounds to get encryption correct.
- Had some legacy issues.
- Was concerned about SP.
- It was not being maintained, no one was using it.
- Turned it off.
- For Error URL, just needed to find the time to write something.
- Took from enhanced spec. Got it done before July 19
- Nobody likes writing documentation and that's what it feels like.

Comment

- One challenges was when we reached out to SP based on the contact info, we found there was a change in the context,
- We had to reach out several times
- These were mainly inside campus, plus some with an external vendor.

InCommon Staff

- Baseline Expectations triggers people looking through registered services to see if they are still current.
- We are seeing metadata being updated
- Some endpoints data getting cleaned up.

Comment

- Hard to keep data "clean"
- People want to stand up services
- Need to ask, Is anyone using this anymore?

- What happened to this entity?
- Through scanning, we find not available scores, servers offline

Albert

- InCommon operations did three passes of Qualysis SSL scans between April and August 2021
- Number of unavailable keeps decreasing
- Obsolete entities are getting removed
- most are running up to date, except issues where legacy needs to be supported

Another BEV2 Hour is tentatively scheduled in one month

Thank you to all who participated.