LInk to 2020 ACAMP wiki

Where should Baseline go beyond BE2?

Advance CAMP Wednesday Nov18,2020

12:20-1:10 am ET

Room - Arts & Crafts

CONVENER: Albert Wu, Internet2

MAIN SCRIBE: Matthew Economou

ADDITIONAL CONTRIBUTORS:

Albert Wu; Andrew Morgan

# of ATTENDEES: 24

DISCUSSION:

- NIH has requested a new level of security/assurance requirements beyond Baseline. Library/content providers are calling for better end user UX during federated SSO. Can we meet these challenges through BE?
-
- Albert W:
    - CTAB spent last year developing Baseline Expectations version 2.0, but some things were postponed to control the scope of the new version.
    - NIH has started enumerating new requirements around assurance, which aligns with BE.
    - Where should BE head after BE2?
    - Can what NIH asks for be achieved using BE?

- David St.PB:
    - Perhaps there are other expectations that if we adhere to them, it adds to the value proposition of federation.
- Matthew:
    - After MFA is Assurance
    - Equally important to be able to say that the binding between this digital identity and legal identity is strong
    - Baseline can help but technical standards are only part of the solution. Are there procedural or business things we need to do?
    - Is this something that Baseline can help with?
    - Login.gov doesn't provide affiliation
    - LinkedIn and ORCID to get additional signals about a person
- Maarten K:
    - Legal identity proofing services like login.gov lose one's institutional affiliation
- Pal A:
    - Student mobility: Erasmus, Erasmus+, Erasmus without papers
    - Use EIDAS/national ID systems to prove legal identity and use institutional ID to prove institutional affiliations.
    - Not done at every login, only for one-time proofing.
    - In GEANT, that's called "My Academic ID"
    - EIDAS limited to EU, not part of Schengen (which is wider)
- Maarten K:
    - With EIDAS, if another country signals its own national identity system, you're obliged to use it, but there's no obligation to make it available.
- Sumit N:
    - Assuming all researchers affiliated with some institution, and there must be some kind of HR and background checking, no matter what country.
- David L:
    - DoE has similar requirements for proofing the IDs of foreign researchers
- Sumit N:
    - Verification versus validation
    - Verification varies across countries. In U.S., the credit bureaus can do this, for example. Can InCommon provide a verification service?
    - Private players like id.me, Jumio, etc.
    - NIH plans to adopt the REFEDS Assurance Framework
    - If institutions can't do it, can third parties add this capability?
- Pal A:
    - Services can validate national IDs but have no access to revocation lists.
- Albert W:
    - If we're talking about employees, everyone in the U.S. has gone through the I-9 process.
    - How difficult would it be to expose I-9 employee status data via IdM infrastructure?

    - Still have loopholes in the form of contractors, etc.
    - Estonia proves identity via banking.
- Chris W:
    - If existing REFEDS Assurance Framework (RAF) can't meet an SP's needs, the SP should hire a service for additional identity proofing.
    - eVerify should meet Espresso, maybe even IAL3?
    - Could InCommon or CTAB ask federations to map their country's ID proofing methods to existing RAF levels?
    - We work in places where nothing like this exists.
- Albert W:
    - CTAB could say if you did an I-9, you can use this level from RAF
- Chris W:
    - What do you do with researchers who are here on their own fellowship?
    - They aren't being paid by any U.S. institution, so no Social Security Number and thus no U.S. government credentials (badge, username, password) because no way to do a background check.
    - Mapping things in RAF could identify areas for improvement in version 2.
- Pal A:
    - The same type of mapping should be "easy" for European countries.
    - We need to find a way that works well for Africa, too.
- Kyle L:
    - IAL3 does require verification by an authorized and trained corp. Rep.
- Sumit N:
    - Likes the idea of having some kind of mapping.
    - Even in Africa, there's some kind of institutional certification that happens, so if we can recognize that process and clearly map that to a RAF profile, that would be a big win.
- Albert W:
    - Bake in mapping of assurance frameworks into interfederation agreements.
    - Do we think Assurance is the next BE target?
    - If so, at least the IdP side is going to have to develop proper ID assurance procedures, so what does that mean?
- Pal W:
    - Nothing happens at the IdP level without SPs demanding change, so glad NIH demands it.
- Chris W:
    - Serious concern that commercial providers and commercial software providers cannot meet these requirements, including the REFEDS Assurance Framework.
- Albert W:
    - From a tooling perspective, the attribute release for RAF should be easy even for commercial services.
    - What might be hard is the underlying business process.

    - Different from MFA, which makes use of a SAML signalling component (AuthnContextClassRef).
- Sumit N:
    - TOTP solutions for second authn factors that can cater to all partners?
- Brett B:
    - A number of institutions are working on that, e.g., Duke's WebAuthn stuff for the Shibboleth IdP
    - eduPersonAssurance attribute release is easy
    - Do we need to adjust attribute release based on entity categories, etc?
    - Disheartening to heard the DoD and NIH we going in different directions (NIH already started this chain of communication to have a cohesive messaging)
- Pal:
    - Big SP in Europe that wants MFA - we have exactly the same problem with commercial entities here (how to signal)

Has R&S been solved?
Chris W: Needs updating before we adopt it in BE3 - identifiers, for example
Albert: TAC has been trying to decide what to do with Deployment Profile and identifiers

Summary:
Albert: MFA and Assurance needs to be topics for CTAB going forward
How to implement it in various pieces of SAML software?