Link to 2024 ACAMP Wiki

Advance CAMP Fri. Dec 13, 2024

Room - II

Session Title: **From Shibboleth to Entra ID**

CONVENER: Tommy (SMU)

MAIN SCRIBE(S): Gail & Jessica

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 20

DISCUSSION:

Tommy (SMU): Entra will do authn, shib will stay and federation
Kellen: 1000 sps in shib, 1000 in entra, how do we clean this up, mgmt wants entra, but what about federation
Jan (UNC-Chapel Hill): running both, use Shib when you can, otherwise oidc with Entra. Paying twice for MFA – Duo, MS MFA
Chris: there's a limit to the number of SPs an Entra tenant can handle, MS has a page that outlines the limits
Colin (University of Washington) - several different IdPs, some Shib, some not, central Entra ID registration set policy where users can easily import apps into the Gallery, 4000-5000 in registry, and 4000-500 not acknowledged, some setup in Entra because easy (but limited attribute release), why paying for 2 MFAs?
->Different policies: Shib required interactions with IAM team, with Entra users are able to have access
-> MS recommended to the Windows team that they encourage folks to use them instead of Shib
Jeff Williams (Greensboro): proxying (Shib does authn) to Azure pre-pandemic, have now swapped, now using azure mfa solely and moved away from Duo, people think we have one IdP

now, you have to be really observant to see the Shib page, shib translates Entra mfa assertion to REFEDS
Tommy: You can register Duo with EntraID directly, this is what we've done, looking for past experiences on what that cutover looks
Chris: EntraID wants to be the only platform, there are limitations, does not do REFEDS MFA. But, if you allow "remember me", Entra honestly reports pw-only login
Patrick (Cirrus Identity): Difference in how Duo is integrated, you won't always get what you want
Clay (RIT): Google for students, 900 in Entra ID, not all users are in EntraID, hit for users

Theme: multiple MFA licensing contracts, it can get expensive. Multiple login experiences.

Kellen: What happens if you have a problem getting to Entra, how do you login to local resources? Health services can't be in this position.
Jeff: As more services have moved to the cloud, these kinds of outages are accepted by the community, like a weather event, folks understand the systems go down and will be back up
Kellen: What about things like student health? This kind of outage would be a really bad situation. Idea about having ability for Shibboleth to handle it, certain relying parties can go to authn backup.
Jeff: General risk for today's cloud environment.
Chris: Business continuity patterns, break the glass kind of conversation, phrase it as a business continuity question, knit adaptive behavior into your architecture, all-cloud MFA and required MFA is also a risk here and you would have to toggle it
Jan: UNC-CH has a UNC-CH option for campus-specific MFA, not REFEDS MFA
Kellen: No on-prem MFA solution, would need to roll out an on-prem MFA solution
Jeff: What value is this for the cost? Do you just accept the risk and fail open?
Colin: Make sure your hospitals carry the risk of failing open rather than campus. Healthcare in our state can be impacted, or attacked by this use case.
Kellen: Question for Clay about Duo passwordless MFA, is anyone using this pervasively>
Clay: Hasn't added OIDC to Shib IdP yet, if someone wants OIDC then they do Duo, app has a really long remember me time, struggle for the 2-3 apps that have been integrated this way, front Duo passwordless with Shib
Chris: multiple services, MS itself, to offer that passwordless option
Kellen: passkeys are only supported with MS Authenticator app, yet another app, Duo+Authenticator app

Jan: VPN has on-prem custom authn option, instead of MFA twice they conditionally prompt for MFA for VPN, 8-10 people IAM team
Kellen: IAM team only does IGA and Grouper, they are 12, about another 20 across campus to handle Shib and Azure
Clay: team of 9 people
Jeff: we have team of two

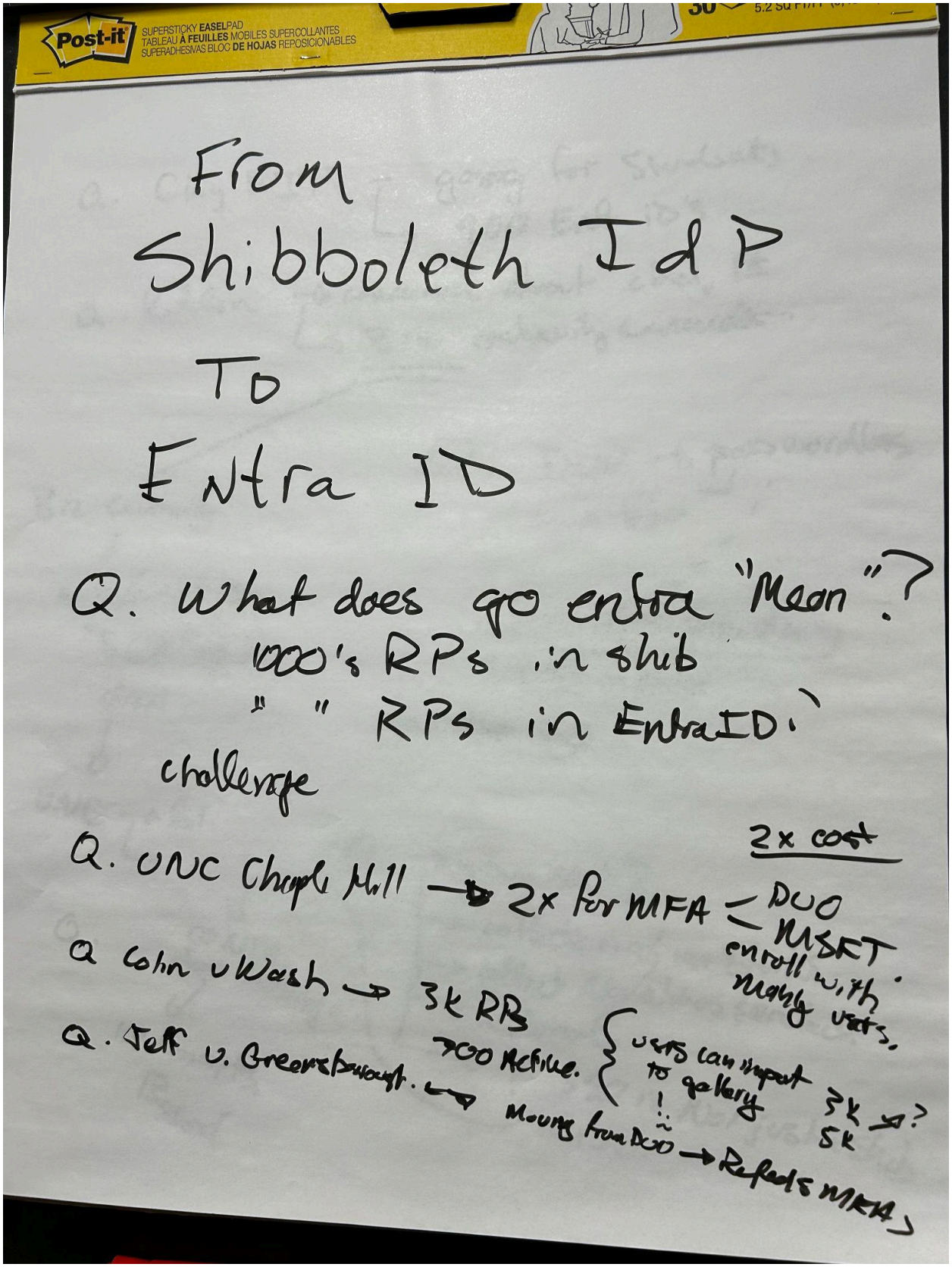
Actions to take:

1) Business Continuity
2) Understanding of Techniques
3) User Stories - Would like something like grouper use cases, here's how our campus can do it, would like names, narratives, we can figure out the technical, it's the higher level discussion; looking for articulation of problems and use cases, include rational and consequences of decisions
4) SSO is not Shib
5) 101 Concepts, base input material

Kellen: Where should this information live? Not necessarily in the Shib wiki.
Colin: SSO is not a Shibboleth conversation for Internet2, it is part of it; most useful info this week are the use cases was CERN conversation because they needed to remove Microsoft for very unique reasons and it was a challenge
Kellen: Would like something IDPro-like in I2-language with stories and documentation, something that would not fit in a product wiki, something like Grouper Deployment Guide; Where do Azure Groups fit into a Grouper-like concept
Chris: Cost is not the initial creation of these docs, it's the sustainability

Next steps:

1. Take it to the Architects group.
2. For the 101 Concepts, see if we can tie it into BaseCAMP (need to make sure everyone can access)


Post-it
SUPERSTICKY EASELPAD
TABLEAU À FEUILLES MOBILES SUPERCOLLANTES
SUPERADHESIVAS BLOC DE HOJAS REPOSICIONABLES
From
Shibboleth IdP
To
Entra ID
Q. What does go entra "Mean"?
1000's RPs in shib
" " RPs in EntraID.
challenge
2x cost
Q. UNC Chapel Hill → 2x For MFA < DUO
< MSFT.
enroll with
many users.
Q Colin v Wash → 3k RP
700 Active.
Q. Jeff v. Greensboro. → Moving from DUO → Refuses MFA
users can import
to gallery
!
3k → ?
5k

Q. Clay RIT
- goog for students
- 900 Ent ID's

Q. Kellen → concerned about clock ☆
- Biz continuity concerns.

Biz Continuity
↓
exit / accept the "SLA" of the cloud.
↓
UNC → fail

Q. DUO → passwordless.
- RIT
- passwordless providers
  - AD on prem.
- passwordless App.

Q. → Where next?
- collection of user stories
- collect Narratives & extract.
- Rationale
- ? SSO is Not just a Shib convo.

Q. CONVO. about the things.
↓
101 concepts.
Based.