§ Link to 2022 ACAMP Wiki

Advance CAMP Thu. Dec. 8, 2022

Room - 5

Session Title: NIH Adoption of REFEDS MFA Profile/REFEDS MFA Profile v1.1 Consultation

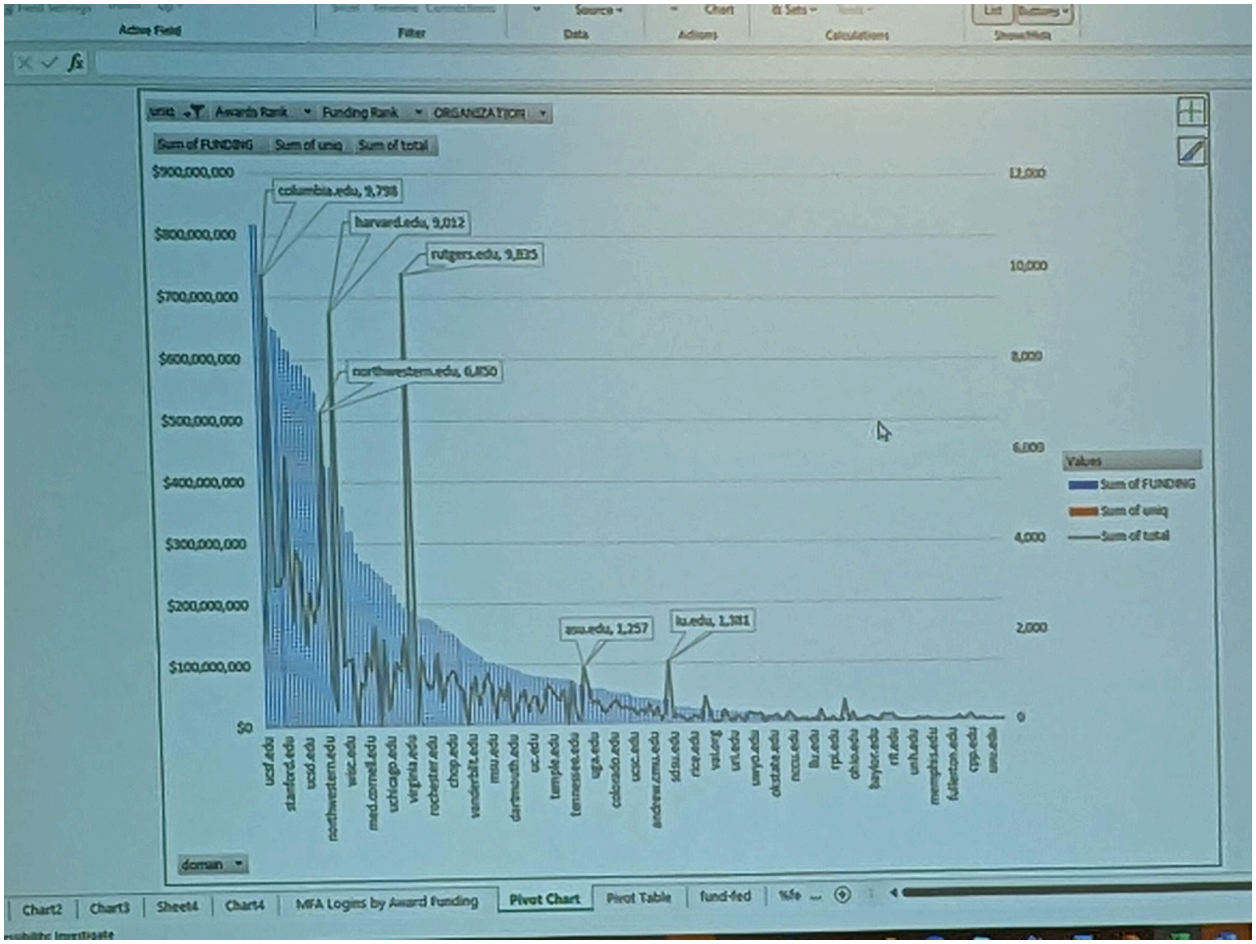
CONVENER: Jeff Erickson, NIH

MAIN SCRIBE(S): Derek Simmel <dsimmel@psc.edu>, Joanen Boomer
ADDITIONAL CONTRIBUTORS: Fredrik Domeij

# of ATTENDEES: 30

DISCUSSION:

We front login for ERA, team was saying we need MFA. They didn't actually ask about federation, just said we're going to use login.gov. Yes, Federation uses MFA profile, but it will take time for adoption.



Test page to determine what you need to send back for the MFA signal at https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx.

Graphic with awards by $$ and who is using federated MFA (see image above):

- 196/~2400 (<10%) are using MFA profile. How to encourage greater adoption??
- Blue bar graph indicates total funding received from NIH at the institution.
- Grey line indicates % of authentications employing MFA.
- Users at many institutions that do support the MFA profile are not yet authenticating with MFA - why is this? - Do users not realize/value using their federated institutional ID + MFA to authenticate at https://public.era.nih.gov/commonsplus/public/login.era ?
- Some institutions, e.g., Columbia and UNC, appear to have a high percentage of users that use their MFA-enabled IDs to authenticate - what are they doing differently to encourage this high level of participation?

- On the https://public.era.nih.gov/commonsplus/public/login.era web interface, the first (top, left) authentication entry is login.gov, with institutional federated ID login available below it - does this imply the preferred method for authentication?

There are 400+ web front ends at NIH - not all require MFA login.

What can we collectively do to leverage federated MFA? What has gone right with this, what could we do better, how can we help?

Liaison with research community messaging is not concerned with using institutions credentials, just get a federal login.

It seems NIH centric, but it's not only for us. Is there not communications across universities.

Swedish Access Federation, SWAMID
If you are running ADFS servers you can use ADFS Toolkit to implement REFEDS MFA.ADFS Toolkit supports Azure MFA or Duo and more. See more here:
https://github.com/fedtools/adfstoolkit

John - Univ of Maryland - we are requiring MFA for all fac/staff/stu. Very easy to do with Shib. But things like Okta do not yet support REFEDS MFA.

Is the challenge of adopting this, is t b/c most people are not doing MFA at all or they are not signaling MFA?

Mark Rank, Cirrus - For a lot of his customers, they are moving to Azure/Okta to deploy MFA. Cirrus/Unicon offer products that will bridge gateway/proxy commercial providers and handle the signaling. They both signal MFA, it's just transforming it into the REFEDS MFA profile.

U of Washington - drivers, but they only just this year started requiring it for students. Now all users are subjected to that. That's new, if they are researchers, now they have multiple MFA accounts, that's a driver to not have to do login and multiple MFA.

NIH is just the first to do it, but NSF and NASA are looking to do this too. NIH talked to NSF, their approach is similar to NIH, it's just a matter of time.

M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf) talks about a new mandated for people who didn't read the guidelines from 2017, we're finally getting around to doing what we should have been doing for some time. These mandates affect across the board, i.e. police to FBI info. All agencies that touch external data will be required to enforce MFA - else they will lose access.

Working with a large number of researchers: they don't want to waste their brain power on this. So if they have another method, they are going to keep using it until it's not available anymore. So they are going to do the easiest method. Therefore login with their federation-member-institution ID + MFA must be the easiest (and most widely usable) method for them to employ.

Western Ontario Canada - as a Canadian citizen are you supposed to have a login.gov account? There are multiple levels; for higher levels/identity proofing, you must be a US Resident. For ERA's purposes it's ok with that lower level of identity assurance. The message here is don't.
In Europe & Sweden, coming from the government, you must do this for all faculty/staff. Starting to create other accounts now can hurt you later on.

Not all MFA meets the REFEDS profile standard.

REFEDS MFA for Shib, easy. But also easy for ADFS running ADFS Toolkit..

Many campuses - do you meet REFEDS standards? I.e. remember me for 30-days will not meet REFEDS. New one says it needs to be done every 12 hours.

UMd rolled MFA out in 3 cohorts - mandated compliance by specific dates.

Driving research staff/principal investigators - how did you do this? Did you know that thing you do to login your email you can login over here.

- Could be word of mouth with researchers.
- A lot of communication from NIH
- Work with InCommon to spread the word

NSF Research.gov (https://identity.research.gov/sso/XUI/?module=nsf&env=prvw&app=portal#login/) features institutional login prominently on that page.

NSF - are these messages getting out and to people on the campuses.
A year ago ERA they had communication on a website in their email.

An easy thing you could do is have federated discovery service available on the page and then have a small link to look at what else I could do.
But it's fewer than 10%.
How do we get IAM staff to get onIboard. Is Azure/Okta hard? Yes, it is a challenge, there are solutions out there that make it quasi turn-key.
Issue - Azure authN thru shib

Needing to replace DUO because of costs, so now they need to figure something else out.

Univ of Missouri is working on it now - Shib+Azure. Major issue is not implementing MFA because you want it for your users, but roll out is monstrous: 1000s of users, differently-abled users, helpdesk load.

David K from UK research - the usual observation, I assume there is a high correlation that the people who have not done it yet are not here at TechEx for this week.

Fredrik - fit in with the proofing. New one out for consultation has more specific requirements for services and NIH. Changes:

- Current REFEDs profile doesn't say anything about session lifespan
- Force authN attribute that you can include in SAML assertion, request the IdP to re-enforce an authentication. Both using password and second factor.
    - 2 separate sessions with assertion lifetimes involved
        - In Shib how long is session good for
        - Within Duo how long is that session good for - i don't have a way to pass on a forced authN to Duo.

If I can't implement it, then how does that help NIH.
Affecting policy, the number of NIH researchers on the campus vs. entire community that needs lower standards.

Reason for 12 hour lifetime?
NIST requirements are 12 hours.
Also what is reasonable and how long is the workday.

Kyle - from experience of SIRTIFI channel, get the idea the strategic/c-level they are not always engaged with these topic. Technical challenge - if CIO is not engaged, there needs to be strategic effort on InCommon's side to educate.
Mark - elevating it to the CIO level
University Office of Research through which grants are all processed can influence the provost-level folks to pay for MFA.
? - it's not just CIO, but if Research departments that can push for change at the provost level. This works for high research institutions, but at smaller institutions, this doesn't work as well. It doesn't need to be a friction point.
With browsers, etc. people are being prompted several times a day.
Other issues include switching between browsers and portability across devices.

Services - are they happy with a long authentication sessions? If we don't require support for ForceAuthn in the profile, no one will probably do anything.

Read thru MFA profile v1.1 proposal and comment on the wiki page consultation page. It's important to get it right. https://wiki.refeds.org/display/CON/Consultation%3A+MFA+Profile+v1.1

https://spaces.at.internet2.edu/display/federation/get-nih-ready
Discovery list - is it the same discovery list as ERA and PubMed.
\

- PubMed is different b/c they are collecting information
- This list and ERA is the same. But if you haven't set it up and your institution then user gets an error.

How consistent is this across the NIH platform. ARe you all talking?

- We haven't expanded MFA requirements to other non-ERA applications
- I think expanding, this is coming real soon. System owner will decide

NIH - we want all institutions to send us all identity and MFA. Assurance is the next session.
NIH Check your token site at https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx returns:

- MFA enabled?
- First Name
- Last Name
- ePPN
- e-mail address

- Organization

How should NIH communicate with all the institutions not yet supporting this?

Switching from ERA login.gov to Institutional?
Not simple to switch login from login.gov ID to Federated Inst ID. ERA does their own account linking. They will link to only one MFA mechanism. First one wins. If someone logins with ERA.gov account, then wants to switch to federated login they will need to call the ERA helpdesk.

NIH account linking mechanism works with self-service, but eRA doesn't yet support this.

Regarding the REFEDS MFA Profile v1.1 proposal:

- What is missing?
- What is unreasonable?
- Is 12 hours maximum session lifetime (including “second factor”) too short?
- How long session lifetime can services allow?
- Do services require capability to force renewed authentication (of all factors), i.e. ForceAuthn?

ARTIFACTS / LINKS

Consultation for the REFEDS MFA Profile v1.1:
https://wiki.refeds.org/display/CON/Consultation%3A+MFA+Profile+v1.1

Get NIH MFA/RAF ready: https://spaces.at.internet2.edu/display/federation/get-nih-ready

Does your authentication token return the desired attributes for NIH? Check at:
https://auth.nih.gov/CertAuthV3/forms/eRAcompliancecheck.aspx

White House Memorandum M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf