# National Institute of Health

## MFA REQUIREMENTS

August 27, 2021

UNICON®

# NIH Compliance

## Next Steps to become National Institute of Health compliant

- Release Attributes
  - NIH
  - R&S
  - All of  InCommon
- REFEDS Multi-factor Authentication
  - Confirm the AuthN context configuration
  - To establish the current ‘session’
- LATER: eduPersonAssurance

# Shibboleth IdP

- Are you releasing attributes to NIH Gateway now?
  - If not, no one can be using your IdP for NIH today
    - So nothing will change FOR YOUR IdP on Sept. 15
  - But InCommon would really like you to have your IdP release to R&S
    - Might become a new Baseline Expectation at some point

# Shibboleth IdP

➜ You can look for this in attribute-filter.xml

- Any InCommon registered SPs
  - <PolicyRequirementRule xsi:type="RegistrationAuthority" registrars="https://incommon.org"/>
- Any federation-designated R&S
  - <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" attributeName="http://macedir.org/entity-category" attributeValue="http://refeds.org/category/research-and-scholarship"/>
- Specifically to the NIH eRA Gateway SP
  - <PolicyRequirementRule xsi:type="Requester" value="https://federation.nih.gov/FederationGateway" />

# Shibboleth IdP

➜ MFA Configuration

- Using the MFA flow
- Have Duo (by far most common in higher ed) configured
- Have associated

  **https://refeds.org/profile/mfa**

  with **authn/Duo** and **authn/MFA** in

  - conf/authn/general-authn.xml or
  - conf/authn/authn.properties (in IdP v4.1.x)

# Shibboleth IdP

- ➜ MFA Configuration
  - Have something like this in the MFA logic (this basic pattern is in copy of this file provided in IdP distribution)
    - conf/authn/mfa-authn-config.xml, in checkSecondFactor bean

```
  ....
nextFlow = "authn/Duo";
  ....
    if (mfaCtx.isAcceptable()) {  // if password alone is good enough
        nextFlow = null;
    }
```

# Shibboleth IdP

- ➜ Delegating authentication to Azure AD?

  Then follow Proxy Task 6 in this Shibboleth wiki page:

  https://shibboleth.atlassian.net/wiki/spaces/KB/pages/1467056889/Using+SAML+Proxying+in+the+Shibboleth+IdP+to+connect+with+Azure+AD#UsingSAMLProxyingintheShibbolethIdPtoconnectwithAzureAD-ProxyTask6.HandlingREFEDSAuthnContextRequests(optional)

- ➜ Delegating authentication to some other SAML IdP service? Then talk to Unicon, we can help if you need help.

# Shibboleth IdP

- Then verify with NIH Compliance Check tool

  [https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx](https://auth.nih.gov/CertAuthV3/forms/compliancecheck.aspx)

- Ignore (for now) any messages about not sending any eduPersonAssurance values. *That will be needed in the future, but not for Sept. 15.*

# Apereo CAS

- Requires Apereo CAS SSO Server version 5.1.x+ configured as SAML2 IdP
- Configure an MFA trigger and MFA provider module
- Integrate NIH services or all of InCommon in the Service Registry
- Release the specified attributes or the R&S bundle in the Service definition(s)
- Configure in cas.properties the Refeds MFA authentication context class to your MFA provider

```
cas.authn.saml-idp.authentication-context-class-mappings[0]=https://refeds.org/profile/mfa->mfa-duo
```

# SimpleSAMLphp

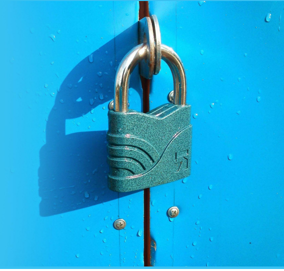
- SimpleSAMLphp
  - Run SimpleSAML as an IdP requires MFA and local attribute release configuration
  - Run SimpleSAML as a proxy back to the IdP requires patch

- MFA
  - Requires a 3rd Party Module or custom development
  - Attribute Release - R&S

- Proxy Patch

https://wiki.refeds.org/pages/viewpage.action?pageId=38895667

# Federation Gateway



Provides multi-entity metadata exchange to establish relationships between SAML IdPs and SAML SPs -- SAML2 Proxy

- ➜ Should be updated to support proxying of ACCR
- ➜ Support of Azure AD MFA mapping

# NIH Down the Road

- Watch for another Webinar & Open Forum Session
  - We’ll present additional NIH requirements
  - We’ll discuss common next steps
  - We’ll answer your questions
- Many branches of government - security needs affect Higher Education

We are happy to setup consulting sessions for more complex needs, please reach out to sales@unicon.net

# Questions? ❯ Answers.

UNICON®

PH: 480.558.2400 FX: 480.558.2320
info@unicon.net | www.unicon.net