Implementing Multi-Factor Authentication on Shibboleth Identity Provider (IdP) using Microsoft 365: Case of NIH Collaboration in Mali and Uganda

Ivan Frank Nsimbi[1], Lloyd Ssentogo[1] , Sidy Soumare[1] , Matthew Economou[2], Christopher Whalen[1,2], Micheal Tartakovsky[2]

[1]Research Data and Communication Technologies, Inc., Garrett Park, MD, USA; [2]Office of Cyber Infrastructure and Computational Biology, National Institute of Allergy and Infectious Diseases, National Institutes of Health, Bethesda, MD, USA;

NIAID

Abstract

The Research and Education FEDerations group (REFEDS) Multi-Factor Authentication (MFA) Profile defines a standard signal Service Providers (SPs) may send to Identity Providers (IdPs) requesting the use of MFA during federated authentication flows. The IdP includes the corresponding signal in its response to indicate that MFA has occurred. The Profile also defines the minimum criteria a second authentication factor must meet for the IdP to claim successful MFA.

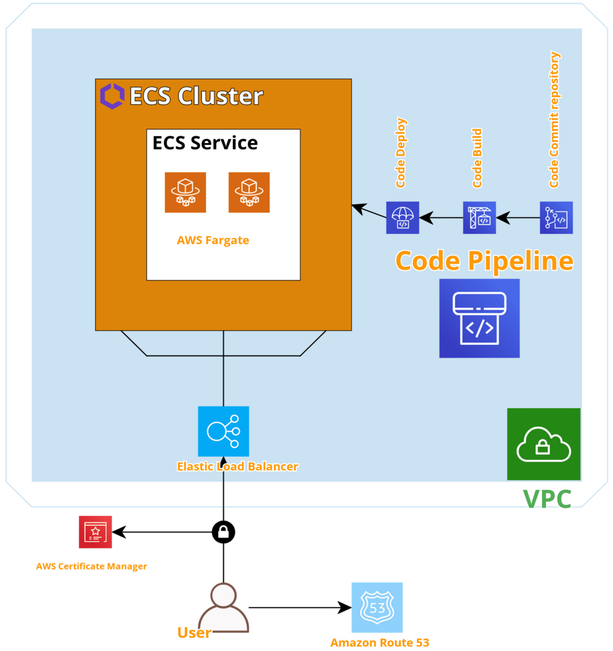
The National Institutes of Health (NIH) announced in June 2021 that it would require MFA for access to some of its resources. As part of the rollout, NIH would require trusted IdPs to support the REFEDS MFA Profile. As more SPs in the Research and Education community continue to require MFA for federated access, IdPs must implement the MFA profile soon.

Requirements

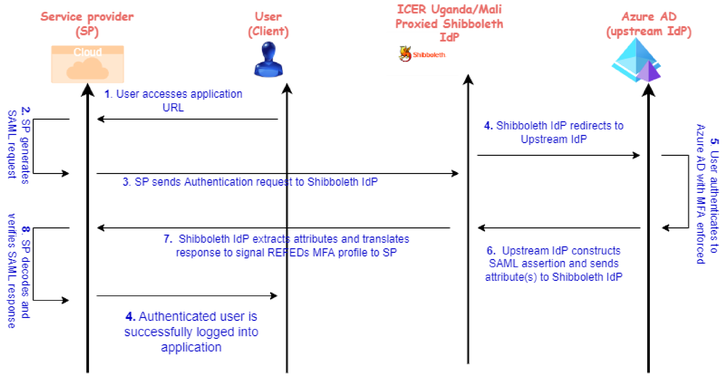
- ✓ A working Shibboleth IdP at version 4.1 or above
- ✓ An active Azure AD tenant that you have administrative control in
- ✓ The ability in Azure AD to create an enterprise Non-Gallery SAML Application
- ✓ A suitable attribute available to both IdPs to use as a "joining" attribute

Architecture & SAML Flow diagrams

Shibboleth IdP running in AWS



Proxied Shibboleth IdP with Azure AD



NOTE: The user will have two sessions; one with Azure AD and another with the Shibboleth IdP

Signaling REFEDS MFA Profile

❖Handling REFEDS AuthnContext Requests

Azure does not currently have a documented way to influence the behavior of the AuthnContext in their SAML assertions.

Shibboleth provides the means to translate proxy requests and responses via **authn/authn-comparison.xml**

❖Update the support matrix for the SAML authentication flow to understand the REFEDS MFA profile

- authn/authn.properties
- authn/authn-comparison.xml

Challenges

- ✓ Low adoption rate to the use of MFA
- ✓ Usability complexity of MFA
- ✓ Users tricked into accepting any MFA requests
- ✓ Some technologies cannot influence the Authentication Context in their SAML assertions
- ✓ Various Service Providers requesting for different Authentication Contexts

REFEDS MFA Profile

An MFA Profile specifies requirements that an authentication event must meet in order to communicate the usage of MFA

The **REFEDS MFA Profile** is a convention for defining basic criteria needed to plausibly claim that an entity has applied Multi-Factor Authentication (MFA) to a subject.

Acknowledgements

❖ **Keith Wessel, IT service manager at University of Illinois at Urbana-Champaign**, for introducing us to the AWS reference implementation of Shibboleth IdP and inspiring the adoption of CI/CD technologies by the NIH ICER program.
❖ **Nate Klingenstein, CEO Signet Identity**, for the use of the SAMLtest.ID testing/validation service.
❖ **Chris Phillips, technical architect at CANARIE**, for documenting the Shibboleth IdP/Azure AD integration and helping the NIH ICER program with the deployment.

Further Information

❖ REFEDS MFA Profile https://refeds.org/profile/mfa
❖ Using SAML Proxying in the Shibboleth IdP to connect with Azure AD
❖ AWS reference implementation of Shibboleth IdP, https://github.com/kwessel/aws-refarch-shibboleth