InCommon Certificate Service SSO+MFA: IdP Setup Requirements

Overview

The goal of the needed Shibb IdP config mentioned below can be simply stated as this:

> *"If the IdP receives a SAML authentication request with 'https://refeds.org/profile/mfa' set as the only authenticationContextClassRef, then it MUST force the user to login with MFA. Optionally, if the IdP receives 'https://refeds.org/profile/mfa' in a list of multiple allowed authentication contexts, it MAY ask the user if they would like to authenticate with MFA."*

The InCommon Cert Service SSO/MFA flow works like this:

1. User clicks federated login link (the link will be provided in the invitation email).
2. User selects IdP from discovery service
3. IdP receives SAML authenticationRequest with 'Password', 'PasswordProtectedTransport', 'http://id.incommon.org/assurance/base-level', and 'https://refeds.org/profile/mfa' set as the allowed/requested SAML authenticationContextClassRef values.
4. IdP optionally asks user if they want to use MFA authentication
5. SP/app receives SAML assertion with user's ePPN.
6. SP/app looks up user's invitation and determines if the user is an RAO.
7. If the user is an RAO, then the SAML authenticationContextClassRef in the received assertion is checked.
8. If the RAO user did not authenticate with MFA, they are sent back to the IdP with only 'https://refeds.org/profile/mfa' set as the allowed/requested SAML authenticationContextClass (since the user was identified as an RAO). Otherwise, the user is a DRAO and they are logged in.

Sectigo Certificate Manager (SCM) SAML SP entityID *(present in the InCommon metadata aggregate)*

https://cert-manager.com/shibboleth

Required Attributes

- Both **eppn** and **email** address are **required**.
  - EduPersonPrincipalName [eppn] (SAML: urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
  - Email address [mail] (SAML: urn:oid:0.9.2342.19200300.100.1.3)
- First and last name are optional.
  - First name [givenName] (SAML: urn:oid:2.5.4.42)
  - Last name [sn] (SAML: urn:oid:2.5.4.4)
- For the initial invitation, the email address asserted by the IdP must match the email address in the invited user's CCM profile. At that point, the user's eppn is stored in their CCM profile.
- Thereafter, only a match on eppn is required to bind the user to their CCM profile.
- The user's eppn can be edited directly in CCM.
- After the initial login, values for email address, first name, and last name received from the IdP will be used to update the related values in the user's CCM profile

Related IdP Configuration Links

- Shibb IdP Configuration for Duo MFA
- Shibb IdP Configuration for MFA Login Flows
- Shibb IdP Resolver Configuration
- Shibb IdP Attribute Filter Configuration

Initial RAO Onboarding (Existing RAOs)

InCommon staff will need to onboard RAOs by sending an invitation email from CCM. Once an institution's IdP is ready, an RAO should send an email to pcaskey@internet2.edu and request such onboarding.

The initial login matches the asserted email address to the email address stored in the CCM user profile.

At that point, the asserted eppn is added to the "IdP User ID" field in the CCM user profile.

All future logins will use asserted values for first/last name and email address to update the respective fields in the CCM user profile.

RAOs can then onboard their DRAOs using the same invitation function (or by manually entering their eppn in CCM). NOTE: Due to a default permissions issue, this will not be functional until 9/13/17.

Onboarding Existing Users

Once logged into CCM, here's how to onboard existing RAOs/DRAOs in your org:

https://spaces.at.internet2.edu/pages/viewpage.action?pageId=115180856 (temporarily restricted, awaiting dev fix on 9/13/17)

Bypassing the Discovery Service

You can bypass the discovery service (for example, if your IdP uses the 'Hide From Discovery' entity tag) using a URL like this (substitute your IdP's entityID where indicated):

*https://cert-manager.com/Shibboleth.sso/Login?target=https://cert-manager.com/customer/InCommon/idp&entityID=**<your IdP's entityID>**&authnContextC*
assRef=Password%20PasswordProtectedTransport%20http://id.incommon.org/assurance/base-level%20https://refeds.org/profile/mfa

Config Contributions

For IdP 3.3.x

```
Change in general-authn.xml:
-- Add new 2fa supported principal to both authn/Duo, and authn/MFA --
<bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/mfa" />

...and then just add a release rule to attribute-filter.xml:
<afp:AttributeFilterPolicy id="Incommon_Certmanager">
  <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://cert-manager.com
/shibboleth" />
  <afp:AttributeRule attributeID="email">
    <afp:PermitValueRule xsi:type="basic:ANY" />
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="givenName">
    <afp:PermitValueRule xsi:type="basic:ANY" />
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="basic:ANY" />
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="basic:ANY" />
  </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

Another 3.3.x contribution

```
<!-- in general-authn.xml -->
<bean id="authn/Duo" parent="shibboleth.AuthenticationFlow"
        p:forcedAuthenticationSupported="true"
        p:nonBrowserSupported="false">
  <property name="supportedPrincipals">
    <list>
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/mfa" />
      <bean parent="shibboleth.SAML1AuthenticationMethod" c:method="https://refeds.org/profile/mfa" />
    </list>
  </property>
</bean>
<bean id="authn/MFA" parent="shibboleth.AuthenticationFlow"
        p:passiveAuthenticationSupported="true"
        p:forcedAuthenticationSupported="true">
  <property name="supportedPrincipals">
    <list>
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:
InternetProtocol" />
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:
PasswordProtectedTransport" />
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:
Password" />
      <bean parent="shibboleth.SAML1AuthenticationMethod" c:method="urn:oasis:names:tc:SAML:1.0:am:password" />
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/mfa" />
      <bean parent="shibboleth.SAML1AuthenticationMethod" c:method="https://refeds.org/profile/mfa" />
    </list>
  </property>
</bean>
<util:map id="shibboleth.AuthenticationPrincipalWeightMap">
  <entry>
    <key>
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="https://refeds.org/profile/mfa" />
    </key>
    <value>2</value>
  </entry>
  <entry>
    <key>
      <bean parent="shibboleth.SAML2AuthnContextClassRef" c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:
PasswordProtectedTransport" />
    </key>
    <value>1</value>
  </entry>
</util:map>




<!-- in idp.properties -->
idp.authn.flows=MFA
```