Identity Provider/OpenID Provider product specific questions

- I run a Shibboleth IdP, what do I need to do to support the REFEDS MFA Profile?
- I run SimpleSAMLphp IdP, what do I need to do to support the REFEDS MFA Profile?
- I run SimpleSAMLphp IdP as SAML Proxy to Azure AD, what do I need to do to support REFEDS MFA Profile?
- I run Microsoft ADFS as my federated IdP. How do I support REFEDS MFA Profile?
- What happens if ADFS tries to handle a REFEDS MFA sign-on without proper configuration?
- I run Microsoft Entra/Azure AD as my federated IdP. How do I support REFEDS MFA Profile?
- I run Apereo CAS, what do I need to do to support REFEDS MFA Profile?
- I run Microsoft Entra/Azure AD as my federated IdP. How do I support REFEDS MFA Profile?

We advise that you review the Shibboleth Knowledge base article Supporting the REFEDS MFA Profile. You will also want to rely on the Shibboleth Multifactor authentication Configuration documentation (V4, V5).

I run SimpleSAMLphp IdP, what do I need to do to support the REFEDS MFA Profile?

NOTE: This answer may be out-of-date, as this contribution has been accepted into the current releases of the product.

For SimpleSAMLphp in Proxy mode, there might be a need to patch the SimpleSAMLphp in order to pass the <AuthnContextClassRef> value from the SP behind the proxy to the upper IdP: https://github.com/simplesamlphp/simplesamlphp/pull/833. The patch has been tested with ELIXIR AAI. Test can be done at https://perun.elixir-czech.cz/refeds-af-demo/.

I run SimpleSAMLphp IdP as SAML Proxy to Azure AD, what do I need to do to support REFEDS MFA Profile?

NOTE: This answer may be out-of-date, as this contribution has been accepted into the current releases of the product.

Similar to the recommendation above there is a way to transform the Azure AD claim of multipleauthentication statement to a REFEDS MFA SAML2 Authentication Context.

Note well: This technique does not take into consideration the Azure AD tenants MFA configuration. Organisations are encouraged to review their configuration against best practices on the factors as they proceed down this path.

For those who use SimpleSAMLphp version 1.19.x as a proxy to delegate authentication to Azure AD, these edits can allow REFEDS MFA to be proxied accordingly:

- Apply tauceti2's patch (https://github.com/simplesamlphp/simplesamlphp/pull/833/files);
- After you have modified the 4 files listed in the previous URL, you need to do some modifications to the code:
  - File SP.php - replace the elseif from line 479 with following:
elseif ($this->passAuthnContextClassRef && isset($state['saml:RequestedAuthnContext'])['AuthnContextClassRef']) { 
    if (isset($state['saml:RequestedAuthnContext']['Comparison']) && in_array($state['saml:RequestedAuthnContext']['Comparison'], array(
        Constants::COMPARISON_EXACT,
        Constants::COMPARISON_MINIMUM,
        Constants::COMPARISON_MAXIMUM,
        Constants::COMPARISON_BETTER,
    ))) {
        // RequestedAuthnContext has been set by an SP behind the proxy so pass it to the upper IdP
        if ($state['saml:RequestedAuthnContext']['AuthnContextClassRef'][0] == "https://refeds.org/profile/mfa") {
            $state['saml:RequestedAuthnContext']['AuthnContextClassRef'][0] = 'http://schemas.microsoft.com/claims/multipleauthn';
        }
        $ar->setRequestedAuthnContext(array(
            'AuthnContextClassRef' => $state['saml:RequestedAuthnContext']['AuthnContextClassRef'],
            'Comparison' => $state['saml:RequestedAuthnContext']['Comparison']
        ));
    }
}

file SAML2.php - add this before line 1137:

if(isset($state['saml:RequestedAuthnContext']) && $state['saml:sp:AuthnContext'] == "http://schemas.microsoft.com/claims/multipleauthn") {
    $state['saml:sp:AuthnContext'] = "https://refeds.org/profile/mfa";
}

in config.php and authsources.php

'proxymode.passAuthnContextClassRef' => true,

Credit: Thanks to Dumitru Motelica of Teluq.ca, member of the Canadian Access Federation.

I run Microsoft ADFS as my federated IdP. How do I support REFEDS MFA Profile?

To support REFEDS SFA and MFA ADFSToolkit needs to be used. Since version 2.1.0 (May 2022) REFEDS SFA and MFA is supported by installing a custom-built Authentication Provider, based on Microsoft's plugin architecture for Custom Authentication Methods.

Minimum requirements to take advantage of this work are to be on Server 2016, have a MFA technology in place, and ADFSToolkit v2.1.0 to be ready to take advantage of this emerging capability and encourage sites to come current to best take advantage of it.

What happens if ADFS tries to handle a REFEDS MFA sign-on without proper configuration?

NOTE: This answer may be out-of-date.

ADFS without any enhancements only recognizes the following AuthenticationContextClassReferences:

- urn:oasis:names:tc:SAML:2.0:ac:classes:Password
- urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
- urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
- urn:oasis:names:tc:SAML:2.0:ac:classes:X509
- urn:federation:authentication:windows
- urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

Custom values cannot be added. If the request has some other authentication context, the following error is displayed:
MSIS7102: Requested Authentication Method is not supported on the STS.

ADFS supports MFA which can be configured as mandatory for some users or SPs but that does not rely on what is in the incoming authentication requests.

In the Authentication responses, custom information on authentication can be mounted on normal attributes but not on the authentication context. So the following is possible (albeit conflicting with the REFEDS MFA Profile):

```xml
<AuthnContext>
  <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef>
</AuthnContext>

<Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
  <AttributeValue>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AttributeValue>
  <AttributeValue>https://refeds.org/profile/mfa</AttributeValue>
  <AttributeValue>http://schemas.microsoft.com/claims/multipleauthn</AttributeValue>
</Attribute>
```

(Credits to Toni Sormunen and Pål Axelsson for this report)

I run Microsoft Entra/Azure AD as my federated IdP. How do I support REFEDS MFA Profile?

Microsoft Entra does not support signalling using REFEDS MFA Profile. Microsoft offers a series of suggested solutions to integrate Azure AD with multilateral federations:


I run Apereo CAS, what do I need to do to support REFEDS MFA Profile?

Apereo CAS has the capability of supporting REFEDS MFA, please see this reference here for DUO with CAS.