MFA/SFA with ADFS

Credits to Toni Sormunen and Pål Axelsson for this report.

REFEDS Assurance Framework

REFEDS Assurance Framework can be easily supported by just populating another custom attribute eduPersonAssurance.

REFEDS MFA/SFA authentication contexts

REFEDS SFA and MFA cannot be supported by ADFS acting as a SAML IdP. In SAML authentication requests ADFS recognizes only 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 REFEDS MFA/SFA specifications):

```
<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>
```