How to request authentication contexts

These examples demonstrate how REFEDS authentication profiles are presented in the SAML 2.0 and OpenID Connect protocol flows

- REFEDS Multi-Factor Authentication (MFA) Profile (https://refeds.org/profile/mfa)
- REFEDS Single-Factor Authentication (SFA) Profile (https://refeds.org/profile/sfa)

SAML authentication contexts

The XML namespaces used in the examples:

- `samlp="urn:oasis:names:tc:SAML:2.0:protocol"`
- `saml="urn:oasis:names:tc:SAML:2.0:assertion`

Example 1: An SP requests MFA

An SP requests MFA (Comparison attribute present):

```
<samlp:RequestedAuthnContext Comparison="exact">
   <saml:AuthnContextClassRef>https://refeds.org/profile/mfa</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

An IdP responds MFA:

```
<saml:AuthnContext>
   <saml:AuthnContextClassRef>https://refeds.org/profile/mfa</saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Alternatively, an IdP responds that it cannot satisfy the request:

```
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext”/>
</samlp:Status>
```

Example 2: An SP prefers MFA but accepts SFA

This is NOT supported by the SAML standard. See the FAQ for alternatives.

OpenID Connectr acr claims

Example 1: An RP requests MFA

An RP issues a claims request, with “essential”:true qualifier as defined in [OIDC Core, section 5.5]:

```
 {
   "id_token":
    {
     "acr": {"essential": true,
             "value": "https://refeds.org/profile/mfa"}

    }
  }
```

An OP responds with an ID token indicating MFA:

```
 {
   "iss": "https://server.example.com",
   "sub": "24400320",
   "aud": "s6BhdRkqt3",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970,
   "auth_time": 1311280969,
   "acr": "https://refeds.org/profile/mfa"
  }
```

Alternatively, an OP responds to the client that it cannot satisfy the request:

```
 HTTP/1.1 302 Found
  Location: https://client.example.org/cb?error=invalid_request&error_description=The%20specified%
20authentication%20context%20requirements%20cannot%20be%20met%20by%20the%20responder.&state=af0ifjsldkj
```

> *N.B. Currently there is no standard error code to signal OP’s inability to satisfy the requested authentication context. A dedicated error code may be later published by competent specification bodies.*

Example 2: An RP prefers MFA but accepts SFA

An RP issues a claims request with a list of authentication contexts in the order of preference and “essential”:true qualifier as defined in [OIDC Core, section 5.5]:

```
{
  "id_token":
   {
    "acr": {"essential": true,
           "values": ["https://refeds.org/profile/mfa",
                      "https://refeds.org/profile/sfa"]}

   }
 }
```

An OP responds with an ID token indicating SFA:

```
{
  "iss": "https://server.example.com",
  "sub": "24400320",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "auth_time": 1311280969,
  "acr": "https://refeds.org/profile/sfa"
 }
```

Note: according to the and OpenID Connect specification, an OP can present only one authentication context in the response.