Integrációk

- EntraID in eduID.hu
- AAI AzureADasAuthsource
- MediaWikiShibboleth
- ElsevierSP
- GoogleAuth

EntraID in eduID.hu

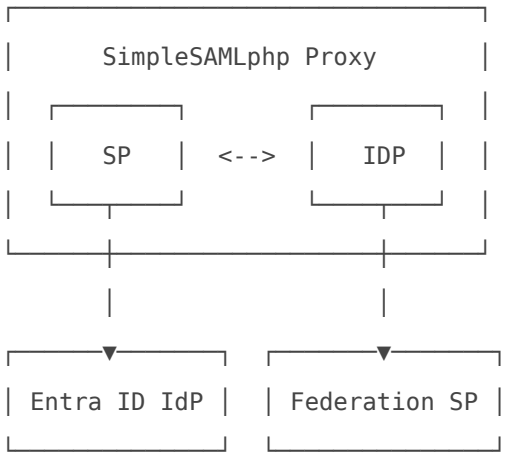
Overview

This document explains how to configure SimpleSAMLphp so that it uses Microsoft Entra ID as the authentication authority (Identity Provider) and then acts as a SAML Identity Provider (IdP) to external federated Service Providers (SPs). This pattern is commonly known as an **authentication proxy** or **IdP proxy**.

In plain terms:

- End users authenticate against **Entra ID**.
- SimpleSAMLphp receives this authentication and optionally enriches or transforms attributes.
- SimpleSAMLphp then issues SAML assertions to federation partners or internal applications.

The proxy setup looks like this:



Configure a SimpleSAMLphp SAML 2.0 Service Provider

To configure SimpleSAMLphp as a SAML 2.0 Service Provider, a new authentication source must be defined in the file `config/authsources.php`. This authentication source represents SimpleSAMLphp in its SP role towards Entra ID and is used to publish SP metadata.

The following example shows a minimal configuration suitable for use with Microsoft Entra ID:

```
$config = [
    /* ... */
    /* An authentication source that can authenticate against SAML 2.0 IdPs. */
    'entraid-sp' => [
        'saml:SP',
        // The entity ID of this SP.
        'entityID' => 'https://proxy.example.org/simplesaml',
        // The entity ID of the IdP this SP should contact.
        'idp' => 'https://sts.windows.net/<your-entra-tenant-id>/'
        'name' => ['en' => 'Microsoft Entra ID'],
        // certificates
        'certificate' => 'server.crt',
        'privatekey' => 'server.key',
        'privatekey_pass' => 'YourPrivateKeyPassphrase', /* you encrypt your private key,
right? */
        'authproc' => [
            /* authproc rules*/
        ],
        // fine tuning the auth source for Entra ID
        'sign.authnrequest' => true,
        'sign.logout' => true,
        'proxymode.passAuthnContextClassRef' => true,
        'disable_scoping' => true,
        'signature.algorithm' => 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256',
    ],
],
```

Configure SimpleSAMLphp SAML 2.0 Identity Provider

In order for SimpleSAMLphp to issue SAML assertions to downstream Service Providers, it must be configured as a SAML 2.0 Identity Provider. This configuration is defined in the file `metadata/saml20-`

`idp-hosted.php`.

The IdP configuration references the previously defined authentication source, effectively chaining authentication to Entra ID.

```
$metadata['http://proxy.example.org/idp'] = [
    /*
     * The hostname of the server (VHOST) that will use this SAML entity.
     *
     * Can be '__DEFAULT__', to use this entry by default.
     */
    'host' => '__DEFAULT__',
    // X.509 key and certificate. Relative to the cert directory.
    'privatekey' => 'server.pem',
    'privatekey_pass' => 'YourPrivateKeyPassphrase',
    'certificate' => 'server.crt',
    /*
     * Authentication source to use. Must be one that is configured in
     * 'config/authsources.php'.
     */
    'auth' => 'entraid-sp', // proxy to Microsoft Entra ID
    'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
    'authproc' => [
    ],
];
```

Create a new Enterprise Application in Entra ID

1. Create a new Enterprise Application

A new **Enterprise Application** must be created in the Entra ID portal to represent SimpleSAMLphp in its role as a SAML Service Provider. This can be done by navigating to the **Enterprise applications** section of the Entra ID portal and creating a new application. During creation, the option to create a custom application that is not found in the gallery should be selected. A descriptive name and also select *Integrate any other application you don't find in the gallery*.

2. Configure SAML-based Single Sign-On

After the application has been created, SAML-based single sign-on must be enabled. This is done by opening the application, navigating to the **Single sign-on** section, and selecting **SAML** as the sign-on method. The trust relationship between Entra ID and SimpleSAMLphp is established by uploading the SAML 2.0 SP metadata generated by SimpleSAMLphp. The metadata upload automatically populates the basic SAML configuration, including the entity ID and assertion consumer service URL.

3. Download Entra ID Federation Metadata

To finalise the SimpleSAMLphp side of the bilateral trust relationship between your Entra ID tenant and SimpleSAMLphp, copy your Enterprise Application's *App Federation Metadata*. Using SimpleSAMLphp's Metadata Converter (found on the *Federation* tab of SimpleSAMLphp's admin portal), convert your App Federation Metadata to SimpleSAMLphp's native PHP format. Once you have the converted metadata, paste it into the `metadata/saml20-idp-remote.php` file.

4. Configure Attribute Claims Rules

Attribute and claim mappings can be adjusted in the Entra ID application to ensure that the required user attributes are released to SimpleSAMLphp. These attributes will later be available for transformation, filtering, or enrichment before being sent to downstream Service Providers.

Attribute Mapping and Transformation

When authenticating against Microsoft Entra ID, user attributes are returned as SAML claims using Microsoft-specific or WS-Federation-style claim URIs. In most federation environments, these claims must be mapped to standard SAML or eduPerson attribute names before they are released to downstream Service Providers.

SimpleSAMLphp performs attribute mapping through authentication processing filters. Mapping rules are applied in the `authproc` section of the authentication source that represents Entra ID, ensuring that attributes are normalized as soon as they enter SimpleSAMLphp. These mappings can either reuse
[https://github.com/simplesamlphp/simplesamlphp/blob/master/attributemap/entra2name.php built-in attribute maps provided] by SimpleSAMLphp or be defined explicitly using custom rules.

Here is an example of using `core:AttributeMap` processing filter:

```
'authproc' => [
    /* ... */
    60 => [
        'class' => 'core:AttributeMap',
        /* there are several versions of the userprincipalname claim, you only need the one
you use */
        'http://schemas.xmlsoap.org/claims/UPN' => 'eduPersonPrincipalName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn' =>
'eduPersonPrincipalName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' =>
'eduPersonPrincipalName',
        /* other possible attributes */
        'http://schemas.xmlsoap.org/claims/CommonName' => 'displayName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'givenName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'sn',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' => 'mail',
        'http://schemas.microsoft.com/ws/2008/06/identity/claims/groups' => 'memberOf',
    ],
    /* ... */
],
```

or

```
'authproc' => [
    60 => [
'class' => 'core:AttributeMap',
'attributemap' => 'entra2name',
    ],
],
```

Once mapped, attributes can be further filtered, enriched, or selectively released by additional authentication processing filters before being issued by the proxy IdP.

Configure SimpleSAMLphp to Use Entra ID as an Authentication Source

With the Enterprise Application configured, SimpleSAMLphp must be instructed to use Entra ID as its authentication source. This is done by setting the IdP entity ID in the entraid-sp authentication source to the Entra ID tenant identifier.

```
'idp' => 'https://sts.windows.net/<your-entra-tenant-id>/',
```

This configuration causes SimpleSAMLphp, acting as a Service Provider, to redirect authentication requests to Entra ID. After importing the Entra ID metadata, the corresponding entity ID should be visible under SAML 2.0 IdP metadata on the Federation tab of the SimpleSAMLphp admin interface.

Testing

You should now be able to go to the **Test** tab in the admin portal, log in to your `entraid-sp` authentication source, and be redirected to your Entra ID application's login page. Once logged in, it is worth verifying that SimpleSAMLphp is correctly receiving the attributes from Entra ID.

Sources

- https://nathansenblog.wordpress.com/2021/02/23/azure-ad-single-sign-on-with-simplesamlphp
- https://safire.ac.za/technical/resources/configuring-simplesamlphp-to-use-entra-id

AAI AzureADasAuthsource

Amennyiben Azure AD-ban tároljuk a felhasználói adatokat, úgy lehetőség van azt azonosítási forrásként is használni. A SimpleSAMLphp oldalon leírt telepítés után az alábbiak elvégzésére van szükség:

(ez csak egy példakonfiguráció, természetesen el lehet ettől térni)

Teendők SimpleSAMLPHP (SSP) oldalon

Keressük ki az Azure AD-ból a Tenant ID-t. A beállítás során erre *TenantID*-val fogunk hivatkozni, oda minden esetben ezt az azonosítót kell behelyettesíteni. Az azonosítót jelenleg a https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview oldalon keresztül lehet beszerezni (Forrás: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant)

A *DOMAIN* helyére a használni kívánt scope-ot szükséges behelyettesíteni (pl intezmeny.hu)

config/authsources.php fájlba

```
    'default-sp' => [
        'saml:SP',

        // The entity ID of this SP.
        // Can be NULL/unset, in which case an entity ID is generated based on the metadata
URL.
        'entityID' => null,

        // The entity ID of the IdP this SP should contact.
        // Can be NULL/unset, in which case the user will be shown a list of available IdPs.
        'idp' => 'https://sts.windows.net/_TenantID_/',
```

```
        // The URL to the discovery service.
        // Can be NULL/unset, in which case a builtin discovery service will be used.
        'discoURL' => null,
        'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
        'simplesaml.nameidattribute' => 'eduPersonTargetedID',

        /*
         * The attributes parameter must contain an array of desired attributes by the SP.
         * The attributes can be expressed as an array of names or as an associative array
         * in the form of 'friendlyName' => 'name'. This feature requires 'name' to be set.
         * The metadata will then be created as follows:
         * <md:RequestedAttribute FriendlyName="friendlyName" Name="name" />
         */
        /*
        'name' => [
            'en' => 'A service',
            'no' => 'En tjeneste',
        ],

        'attributes' => [
            'attrname' => 'urn:oid:x.x.x.x',
        ],
        'attributes.required' => [
            'urn:oid:x.x.x.x',
        ],
        */
    ],
```

config/config-metarefresh.php fájlba

```
$config = [

    'sets' => [
        'azure' => [
            'cron' => ['hourly'],
            'sources' => [
                [
                    'src' =>
```

```
'https://login.microsoftonline.com/_TenantID_/federationmetadata/2007-
06/federationmetadata.xml',
                ],
            ],
            'expireAfter' => 34560060, // Maximum 4 days cache time (3600*24*4)
            'outputDir' => 'metadata/metarefresh-azure',
            'outputFormat' => 'flatfile',
        ],
    ],
];
```

metadata/saml20-idp-hosted.php

A

```
    'authproc' => [

        10 => [
              'class' => 'core:AttributeMap',
              'azure2name'
        ],

        15 => [
            'class' => 'core:AttributeCopy',
            'eduPersonPrincipalName' => 'schacPersonalUniqueCode',
        ],

        16 => ['class' => 'core:PHP',            'code' => '                $attributes[=
"urn:schac:personalUniqueCode:int:esi:_DOMAIN_:" .
$attributes["schacPersonalUniqueCode"]("schacPersonalUniqueCode"][0])[0];
            ',
        ],

        18 => [
            'class' => 'core:AttributeAlter',
            'subject' => 'eduPersonPrincipalName',
            'pattern' => '/^.*$/',
            'replacement' => '${0}@_DOMAIN_',
            'target' => 'eduPersonPrincipalName'
```

```
        ],

        20 => [
            'class' => 'core:AttributeAdd',
            'eduPersonEntitlement' => array('urn:mace:dir:entitlement:common-lib-terms')
        ],

        22 => [
            'class' => 'core:AttributeAdd',
            'schacHomeOrganization' => array('_DOMAIN_')
        ],

        23 => [
            'class' => 'core:AttributeAdd',
            'schacHomeOrganizationType' =>
array('urn:schac:homeOrganizationType:eu:higherEducationalInstitution')
        ],

// Azure AD-ban célszerű az affilation-t (intézményhez való viszonyt, pl hallgató, oktató,
dolgozó) security group alapján meghatározni. Ezeknek az objektum azonosítóját át fogja adni
az Azure AD, amit könnyen kicserélhetünk a kívánt affilation-re:

        31 => [
            'class' => 'core:AttributeAlter',
            'subject' => 'eduPersonAffiliation',
            'pattern' => '/^_eduID_Dolgozó_GroupID_$/', // _eduID_Dolgozó_GroupID_ értéket
cseréljük a megfelelő Objektum ID-ra
            'replacement' => 'faculty',
        ],

        32 => [
            'class' => 'core:AttributeAlter',
            'subject' => 'eduPersonAffiliation',
            'pattern' => '/^_eduID_Hallgató_GroupID_$/', // _eduID_Hallgató_GroupID_ értéket
cseréljük a megfelelő Objektum ID-ra
            'replacement' => 'student',
        ],

        33 => [
```

```
            'class' => 'core:AttributeAlter',
            'subject' => 'eduPersonAffiliation',
            'pattern' => '/^_eduID_Admin_GroupID_$/', // _eduID_Admin_GroupID_ értéket
cseréljük a megfelelő Objektum ID-ra
            'replacement' => 'staff',
        ],

        34 => [
            'class' => 'core:AttributeAdd',
            'eduPersonAffiliation' => array('member'),
        ],

        35 => [
            'class' => 'core:AttributeCopy',
            'eduPersonAffiliation' => 'eduPersonScopedAffiliation'
        ],

        36 => [
            'class' => 'core:AttributeAlter',
            'subject' => 'eduPersonScopedAffiliation',
            'pattern' => '/^.*$/',
            'replacement' => '${0}@$_DOMAIN_',
        ],

        50 => [
            'class' => 'core:TargetedID',
            'identifyingAttribute' => 'eduPersonPrincipalName',
            'nameId' => TRUE,
        ],

        60 => [
            'class' => 'core:AttributeMap',
            'name2oid'
        ],
        75  => [
            'class' => 'entitycategories:EntityCategory',
            'default' => true,
            'strict' => false,
            'allowRequestedAttributes' => true,
```

```
            'http://eduid.hu/category/registered-by-eduidhu' => [],
            'http://www.geant.net/uri/dataprotection-code-of-conduct/v1' => [
                'urn:oid:2.16.840.1.113730.3.1.241', # displayName
                'urn:oid:2.5.4.4', # sn
                'urn:oid:2.5.4.42', # givenName
                'urn:oid:0.9.2342.19200300.100.1.3', # mail
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.6', # eduPersonPrincipalName
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.9', # eduPersonScopedAffiliation
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.1', # eduPersonAffiliation
            ],
            'http://refeds.org/category/research-and-scholarship' => [
                'urn:oid:2.16.840.1.113730.3.1.241', # displayName
                'urn:oid:2.5.4.4', # sn
                'urn:oid:2.5.4.42', # givenName
                'urn:oid:0.9.2342.19200300.100.1.3', # mail
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.6', # eduPersonPrincipalName
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.9', # eduPersonScopedAffiliation
                'urn:oid:1.3.6.1.4.1.5923.1.1.1.1', # eduPersonAffiliation
            ],
        ],

        90 => 'core:AttributeLimit',
    ],

    'simplesaml.nameidattribute' => 'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',

    'attributeencodings' => array(
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.10' => 'raw', /* eduPersonTargetedID with oid
NameFormat. */
    ),

    'sign.logout' => true
];
```

attributemap/azure2oid.php

```
<?php
$attributemap = [
    // displayName
    'http://schemas.microsoft.com/identity/claims/displayname' =>
'urn:oid:2.16.840.1.113730.3.1.241',
    // eppn
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' =>
'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',
    // givenName
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'urn:oid:2.5.4.42',
    // cn
    '://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'urn:oid:2.5.4.3',
    // surname
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'urn:oid:2.5.4.4',
    // mail
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' =>
'urn:oid:0.9.2342.19200300.100.1.3',
    // o & organisation
    'http://schemas.microsoft.com/identity/claims/tenantid' => 'urn:oid:2.5.4.10',
];
```

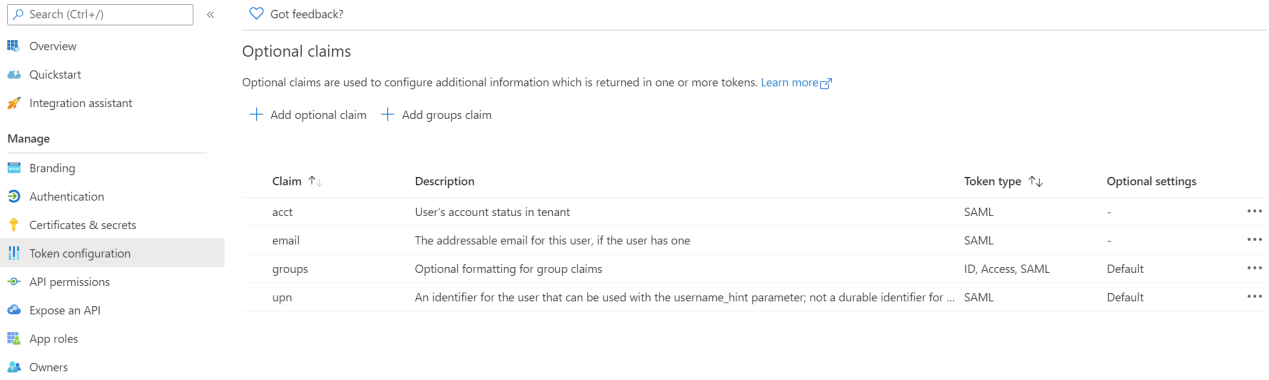
attributemap/azure2name.php

```
<?php
$attributemap = [
    // eppn
    'http://schemas.microsoft.com/identity/claims/objectidentifier' =>
'eduPersonPrincipalName',
    // mail
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' => 'mail',
    // displayName
    'http://schemas.microsoft.com/identity/claims/displayname' => 'displayName',
    // givenName
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'givenName',
    // cn
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'sn',
    // affiliation
    'http://schemas.microsoft.com/ws/2008/06/identity/claims/groups' =>
```

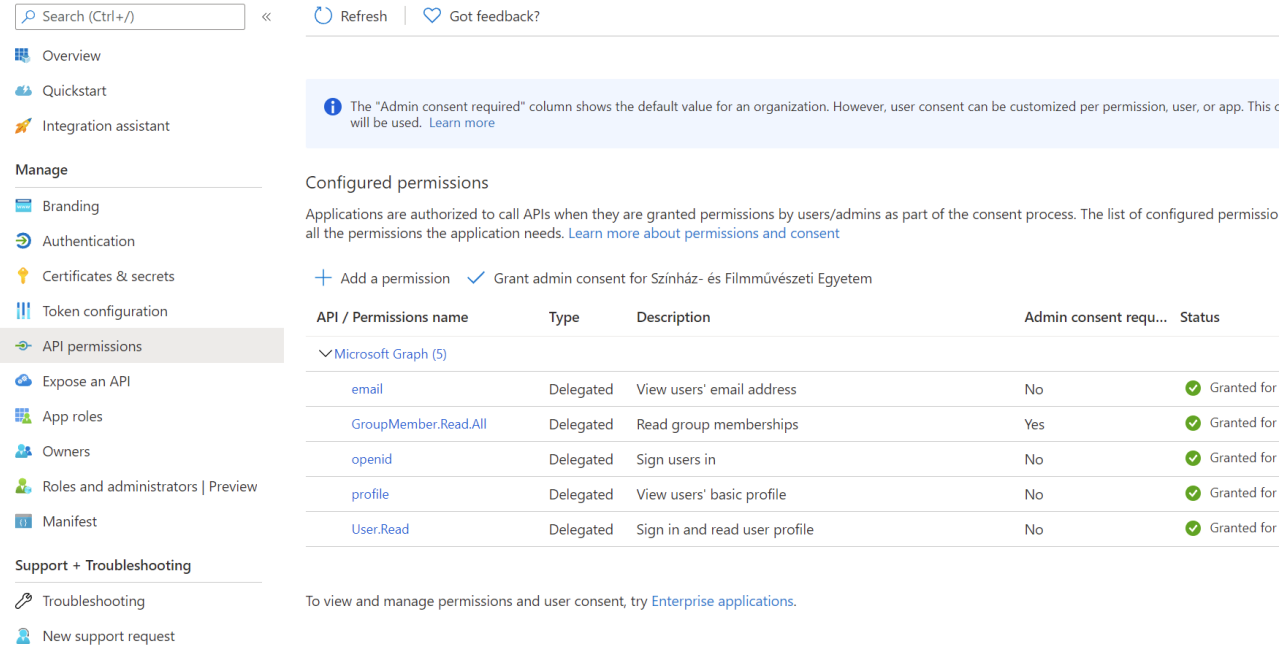
```
'eduPersonAffiliation',
];
```

Teendők Azure AD oldalon

1. A https://portal.azure.com/ oldalon jelentkezzünk be egy adminisztrátori fiókkal
2. Válasszuk az "App registrations"-t
3. "New registration"
4. "Redirect URI (optional)" -nál adjuk meg a telepített SSP default SP címét. Pl: https://idp.*DOMAIN*/simplesaml/module.php/saml/sp/metadata.php/default-sp
5. "Token configuration" # > "Add optional claim"> "Token type"-nál válasszuk a "SAML"-t és jelöljük ki az összes attribútumot, majd, "Add"
6. "Add groups claim", majd mentsük el



7. Állítsuk be az API persmissions-t az alábbi alapján:



Teszt

MediaWikiShibboleth

- Shibboleth Authentication Extension: http://www.mediawiki.org/wiki/Extension:Shibboleth_Authentication
- Shibboleth Authentication Plus Extension: http://www.mediawiki.org/wiki/Extension:Shibboleth_Authentication_Plus

ElsevierSP

Speciális eduPersonTargetedID kiadásának beállítása

Shibboleth IdP alatt

```
vim [/path/to]/shibboleth-idp/conf/attribute-resolver.xml
```

Szúrjuk be az alábbi attribútumdefiníciót, ahol

- a `scope` értéke az intézményi scope (ugyanaz, amit pl. az eduPersonPrincipalName attribútum előállításakor is használ)
- a `sourceAttributeID` értéke a persistent nameID-t előállító attribútum id-je

```
    <!-- Buggy edupersonTargetedId required for Elsevier: -->
    <resolver:AttributeDefinition id="elsevierId" xsi:type="Scoped" scope="niif.hu"
sourceAttributeID="persistentId"
                                  xmlns="urn:mace:shibboleth:2.0:resolver:ad" >
      <resolver:Dependency ref="storedIdConnector" />
      <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
                                 name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="buggy-
eduPersonTargetedID"
                                 xmlns="urn:mace:shibboleth:2.0:attribute:encoder" />
    </resolver:AttributeDefinition>
```

```
vim [/path/to]/shibboleth-idp/conf/attribute-filter.xml
```

Fontos, hogy amennyiben az ajánlásnak megfelelően a Resource Registry által előállított attribute filtert használjuk, akkor ne ezt a dinamikusan frissülő fájlt szerkesszük, hanem az attribute-filter-local.xml-t, és ebben a fájlban végezzük el az alábbi módosításokat.

1. Szúrjuk be az alábbi részletet, amely megmondja, hogy az Elsevier SP számára mely attribútumok adandók ki:

```
    <AttributeFilterPolicy id="buggy-eptid">
            <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value="https://sdauth.sciencedirect.com/" />
            <AttributeRule attributeID="elsevierId">
                <PermitValueRule xsi:type="basic:ANY" />
            </AttributeRule>
            <AttributeRule attributeID="eduPersonScopedAffiliation">
                <PermitValueRule xsi:type="basic:ANY" />
            </AttributeRule>
    </AttributeFilterPolicy>
```

2. A `releaseIDsToAnyone` alapértelmezett szabályt módosítsuk az alábbiakra:

```
    <!--  Release IDs to anyone -->
    <AttributeFilterPolicy id="releaseIDsToAnyone">
        <PolicyRequirementRule xsi:type="basic:NOT">
                <basic:Rule xsi:type="basic:AttributeRequesterString"
value="https://sdauth.sciencedirect.com/" />
        </PolicyRequirementRule>
        <AttributeRule attributeID="transientId">
            <PermitValueRule xsi:type="basic:ANY" />
        </AttributeRule>

        <AttributeRule attributeID="persistentId">
            <PermitValueRule xsi:type="basic:ANY" />
        </AttributeRule>

    </AttributeFilterPolicy>
```

Ez utóbbi módosításra azért van szükség, hogy a mindenki számára kiadható szabványos persistentID ne csapja felül ez Elsevier számára kiadandót.

SimpleSAMLphp alatt

```
vim [/path/to]/simplesaml/metadata/saml20-sp-remote.php
```

Beállítjuk, hogy csak az elsevier SP-je esetén az attribútum előállítás és kiadás folyamatát toldja meg még egy lépéssel. Ehhez szükséges, hogy a fenti fájlba vegyük fel állandó elemként az

Elsevire SP metadatájának kiegészítéseként az alábbi PHP tömböt. Fontos, hogy a tömb egyes elemei előtt szereplő számok magasabbak legyenek, mint az IdP általános feloldási szabályainál megadott számok, de alacsonyabbak, mint a jellemzően a folyamat végén beállított 'name2oid' mappelések.

```
$metadata['https://sdauth.sciencedirect.com/']['authproc'] = array (
               96 => array(
                        'class' => 'core:TargetedID'
               ),
               97 => array(
                       'class' => 'core:AttributeAlter',
                       'subject' => 'eduPersonTargetedID',
                       'pattern' => '/^.*$/',
                       'replacement' => '${0}@intezmenyiScope.hu',
               ),
);
```

A fenti kódrészlet annyit teszi, hogy újragenerálja az alapértelmezett eduPersonTargetedID-t egyszerű formában (csak a stringet, a NameID-s xml struktúra nélkül), majd mögé teszi az intézményi scope-ot. Fontos, hogy a megoldás feltételezi azt, hogy az Elsevier SP metadatájának további részei betöltésre kerülnek pl. a metarefresh modul által.

GoogleAuth

Alapok

A wikiben részletezett többi megoldáshoz képest ez a fejezet kilóg a sorból, hiszen ez a megoldás "a federáción" belül csak egy Identity Providert használ - a google központi kapuját. Ezt bárki használhatja a saját szolgáltatásában (SP) történő felhasználó-hitelesítésére, természetesen annyi megszorítás van, hogy az adott felhasználóknak rendelkezniük kell Google Accounttal (gmail-es e-mail címmel).

A google ekkor 2.0-ás szabványú OpenID protokoll szerint működő OpenID IdP-ként viselkedik, emellett támogatja az OpenID Attribute Exchange 1.0 alapú attribútum kiadást, így ha a felhasználó az autentikáció során hozzájárul a felsorolt adatainak az SP részére történő kiadásához, akkor azt a google ki is adja. (A kiadható attribútumok köre korántsem teljes, lévén jelenleg egyedül az e-mail cím kiadatására van lehetősége az SP-nek)

Beállítás

Az autentikációhoz használt google-végpont a

https://www.google.com/accounts/o8/id

címen érhető el, a megfelelő paramétereket ide kell átadni.

Rendelkezésre álló paraméterek

openid.ns	**Kötelező - a használandó OpenID protokollt definiálja, ajánlott érték: "http://specs.openid.net/auth/2.0"**
openid.claimed_id	Opcionális - a kérelem típusát azonosítja, ajánlott érték: "http://specs.openid.net/auth/2.0/identifier_select"
openid.identity	Opcionális, egy alternatív azonosítót definiál, ajánlott érték: "http://specs.openid.net/auth/2.0/identifier_select"

openid.ns	Kötelező - a használandó OpenID protokollt definiálja, ajánlott érték: "http://specs.openid.net/auth/2.0"
openid.return_to	Kötelező - azt az oldalt definiálja, amelyre a google visszairányít az autentikáció után. Támogatott http és https protokollú visszatérő oldal egyaránt.
openid.realm	Opcionális - azt a domaint definiálja, amelyre a felhasználót a google-el autentikáltatni szeretnénk. Alapértelmezés szerint az openid.return_to-nál megadott honlapra mutat. Amennyiben megadásra kerül, akkor a domainnek mindenképp egyeznie kell az openid.return_to domainnevével.
openid.assoc_handle	Opcionális - részletes ismetető: http://openid.net/specs/openid-authentication-2_0.html#associations
openid.mode	Kötelező - a kérés módját adja meg, a két lehetséges érték: "checkid_immediate" (szinkron kommunikáció) "checkid_setup" (aszinkron kommunkikáció)
openid.ns.ext1	Opcionális (attribútum kiadatáskor kötelező) - ajánlott érték: "http://openid.net/srv/ax/1.0"
openid.ext1.mode	Opcionális (attribútum kiadatáskor kötelező) - ajánlott érték: "fetch_request"
openid.ext1.type.email	Opcionális (attribútum kiadatáskor kötelező) - ajánlott érték: "http://axschema.org/contact/email"
openid.ext1.required	Opcionális (attribútum kiadatáskor kötelező) - ajánlott érték: "email" (Jelenleg csak az email attribútum elérhető)

Minta kérés

Az alábbi kérés igényli az email-cím attribútum kiadását is

```
https://www.google.com/accounts/o8/ud
?openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
&openid.claimed_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select
&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select
&openid.return_to=http%3A%2F%2Fwww.example.com%2Fcheckauth
&openid.realm=http%3A%2F%2Fwww.example.com%2F
&openid.assoc_handle=ABSmpf6DNMw
&openid.mode=checkid_setup
&openid.ns.ext1=http%3A%2F%2Fopenid.net%2Fsrv%2Fax%2F1.0
&openid.ext1.mode=fetch_request
```

```
&openid.ext1.type.email=http%3A%2F%2Faxschema.org%2Fcontact%2Femail
&openid.ext1.required=email
```

Minta válasz sikeres autentikáció esetén

```
http://www.example.com:8080/checkauth
?openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
&openid.mode=id_res&openid.op_endpoint=https%3A%2F%2Fwww.google.com%2Faccounts%2Fo8%2Fud
&openid.response_nonce=2008-09-18T04%3A14%3A41Zt6shNlcz-MBdaw
&openid.return_to=http%3A%2F%2Fwww.example.com%3A8080%2Fcheckauth
&openid.assoc_handle=ABSmpf6DNMw
&openid.signed=op_endpoint%2Cclaimed_id%2Cidentity%2Creturn_to%2Cresponse_nonce%2Cassoc_handle
%2Cext1.mode%2Cext1.type.email%2Cext1.value.email
&openid.sig=s%2FgfiWSVLBQcmkjvsKvbIShczH2NOisjzBLZOsfizkI%3D
&openid.identity=https%3A%2F
%2Fwww.google.com%2Faccounts%2Fo8%2Fid%3Fid%3DACyQatixLeLODscWvwqsCXWQ2sa3RRaBhaKTkcsvUElI6tNH
IQ1_egX_wt1x3fAY983DpW4UQV_U
&openid.claimed_id=https%3A%2F%2Fwww.google.com%2Faccounts%2Fo8%2Fid%3Fid%3DACyQatixLeLODscWvw
qsCXWQ2sa3RRaBhaKTkcsvUElI6tNHIQ1_egX_wt1x3fAY983DpW4UQV_U
&openid.ns.ext1=http%3A%2F%2Fopenid.net%2Fsrv%2Fax%2F1.0
&openid.ext1.mode=fetch_response
&openid.ext1.type.email=http%3A%2F%2Faxschema.org%2Fcontact%2Femail
&openid.ext1.value.email=fred.example%40gmail.com
```

Minta választ sikertelen autentikáció esetén

```
http://www.example.com/checkauth
?openid.mode=cancel
&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
```

Válaszok feldolgozása

A megfelelő kérés elküldése után a rendszer átirányít a google autentikációs oldalára, ahol a felhasználónak meg kell adnia google accounttal kapcsolatos adatait, majd sikeres bejelentkezés után jóvá kell hagynia, hogy a SP részére a google átadja az információt, hogy bejelentkezett ill. az

egyéb attribútumokat, melyeket adott esetben az SP igényelt. Pozitív válasz esetén a google beállítva a megfelelő értékeket meghívja a visszatérő oldalt, ahol a megfelelő GET paraméterek feldolgozásával már SP-hatáskörben irányíthatók tovább a felhasználók.

Külső hivatkozások

- http://code.google.com/intl/hu-HU/apis/accounts/docs/OpenID.html