SimpleSAMLphp

Az alábbi lapon megkíséreljük összefoglalni a legfontosabb lépéseket, melyek általános esetben elegendőek ahhoz, hogy működő SimpleSAMLphp (SSP) alkalmazást állítsunk üzembe.

Telepítés

A leírás a forrásból történő telepítés lépéseit írja le. Az itt részletezetten kívül a SimpleSAMLphp telepíthető Debian (vagy más) operációs rendszer csomagjából, de ebben az esetben ne telepítsunk composerrel third-party (pl. általunk készített) modulokat!

El?készületek

Ahhoz, hogy problémamentesen telepíthessük SSP alkalmazásunkat, az alábbi szoftverkomponenseknek kell működniük szerverünkön.

- PHP futtatására alkalmas webszerver
- PHP környezet (>=5.4)
- A következő PHP kiterjesztéseket engedélyezni kell
  - `date`, `dom`, `hash`, `libxml`, `openssl`, `pcre`, `SPL`, `zlib`
  - LDAP-ból történő autentikáció esetén: `ldap`
  - Adatbázisból történő autentikáció esetén a megfelelő adatbázis-csatolót `mysql`, `pgsql`
  - RADIUS szerveren keresztül történő autentikáció esetén: `radius`
  - Assertion-ök titkosítása esetén: `mcrypt`
  - Memcache használata esetén: `memcache`
  - HEXAA integrációhoz (SP): `soap`

Debian 9 / Ubuntu 16.04 LTS csomagok

```
sudo apt install php php-dom mcrypt php-xml php-mbstring
```

RHEL / CentOS 7 csomagok

A **php-mcrypt** csomaghoz engedélyezni kell az "*epel-release*"-t.

```
sudo yum install epel-release
sudo yum update
sudo yum install php php-dom php-mcrypt php-xml php-mbstring php-common mod_ssl
```

Composer

A **composer** PHP csomagkezelőt is telepíteni kell (akár forrásból, akár csomagból), hogy telepíteni lehessen a SimpleSAMLphp futásához szükséges PHP library-ket.

Letöltés

A GitHubról történő telepítés előnye, hogy a simplesamlphp könnyen frissíthető marad, csak a third party modulokat kell újratelepíteni. Az utolsó stabil verzió számát a

https://simplesamlphp.org/download oldalról tudhatjuk meg.

```
cd /var
git clone
[https://github.com/simplesamlphp/simplesamlphp.git](https://github.com/simplesamlphp/simplesa
mlphp.git)
cd simplesamlphp
git checkout tags/v1.16.2 -b v1.16.2
composer install --no-dev
```

Apache konfigurálás

A webről csak a `/var/simplesamlphp/www` könyvtárat kell elérni. **Tilos** a teljes simplesamlphp könyvtárat a DocumentRoot alá tenni!

```
Alias /simplesaml /var/simplesamlphp/www
<Directory /var/simplesamlphp/www>
  Require all granted
</Directory>
```

Alapbeállítások

Konfigurációs fájlok másolása

Mielőtt aktiváljuk valamelyik főszolgáltatását (IdP,SP...) a telepített alkalmazásnak, néhány beállítást meg kell adnunk a `config/config.php` és `config/authsources.php` konfigurációs fájlokban.

- **config.php** másolása a **config-templates** mappából cp config-templates/config.php config/
- **authsources.php** másolása a **config-templates** mappából cp config-templates/authsources.php config/

A **config.php** és **authsources.php** fájlok másolása utána ellenőrizzük, hogy a SimpleSAMLphp működik-e, a https://example.org/simplesaml oldalon.

Konfigurációs fájlok szerkesztése

Adminisztrációs adatok beállítása

Amennyiben az SimpleSAMLphp kezdőlapja hiba nélkül megjelent, akkor nyissuk meg a **config/config.php** fájl szerkesztésre és végezzük el az alábbi beállításokat.

- **Az "admin" felhasználó jelszavát, mellyel webes felületen keresztül be tud lépni a települő SSP-be.**
  'auth.adminpassword' => 'ujjelszotirdide',
- **Titkosítási feladatokhoz szükséges "salt", azaz véletlenszerűen összeálló karaktersorozat**

  ```
  'secretsalt' => 'randombytesinsertedhere',
  ```

  A karaktersorozat előállításában segíthet az alábbi parancs:

  ```
  tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo
  ```

- **Elérhetőségeket, amely adatok bekerülnek majd a generált metaadatba**

  ```
  'technicalcontact_name'     => 'Gipsz Jakab',
  'technicalcontact_email'    => 'jakab.gipsz@example.org',
  ```

- **Nyelv és időzóna adatok**

  ```
  'language.default'      => 'hu',
  'timezone' => 'Europe/Budapest',
  ```

Az alapadatok megadása után mentsük és zárjuk be a **config.php**-t.

Naplózás beállítása

Alapértelmezetten a SimpleSAMLphp a **syslog**-ba irányítja a naplózást.

Ha fájlba akarunk naplózni, akkor a megfelelő könyvtárhoz biztosítsunk írás jogot a webszerver felhasználónak, és ne felejtsünk el gondoskodni a naplófájlok rotálásáról!

- **log** mappa létrehozása és jogosultság beállítása

  ```
  sudo mkdir log; sudo chown www-data:adm log; sudo chmod 755 log
  ```

- Naplózási szint beállítása a **config/config.php**-ban

```
'debug' => array(
    'saml' => true,
    'backtraces' => true,
    'validatexml' => false,
),
'logging.level' => SimpleSAML\Logger::DEBUG,
'logging.handler' => 'file',
```

A "SimpleSAML\Logger::DEBUG" a legrészletesebb naplózási beállítás, éles rendszernél nem ajánlott csak hiba keresés esetén.

Tanúsítvány készítése

Nem ajánlott a SimpleSAMLphp-hoz és webszerverhez ugyanazt a tanúsítvány használni!

- A SimpleSAMLphp alapértelmezetten a tanúsítványt a **cert** mappában keresi.

```
mkdir cert
```

- Az alábbi paranccsal egy 10 éves self-signed tanúsítvány generálunk a SimpleSMALphp számára.

```
openssl req -new -newkey rsa:2048 -x509 -days 3652 -nodes -out cert/saml-example-org.crt -keyout cert/saml-example-org.key
```

A fingerprint az alábbi módon kérdezhető le a legegyszerűbben

```
openssl x509 -fingerprint -noout -in cert/saml-example-org.crt
```

Telepítés kész

Amennyiben elkészültünk a fenti lépésekkel, úgy a https://service.example.org/simplesaml/ címen elérjük a telepített SSP-nk webes adminfelületét, ahol megejthetjük a további beállítások nagy részét.

Identity Provider (IdP) beállítás

Alapbeállítások

IdP engedélyezése: a **config/config.php** fájlban kell a saml20 idp-t "true"-re állítani.

```
'enable.saml20-idp' => true,
```

LDAP autentikáció

Meg kell adni, hogy az IdP milyen módon azonosítsa a felhasználót, amennyiben alapértelmezés szerint nem engedélyezett modult szeretnénk használni, úgy a megfelelő modult a `modules` könyvtár alatt engedélyezni kell. Az alábbi példában az LDAP alapú azonosítást mutatjuk be, amely külön modult nem igényel, alapértelmezés szerint része a telepített alkalmazásnak.

Javasolt az LDAP-ban egy olyan bejegyzést létrehozni az IdP számára, amely olvasni tudja a felhasználóknak a föderációban használt attribútumait. Az azonosítás alapértelmezett módon a felhasználó nevében történő újra bind-olással történik, így a jelszóhoz nem kell hozzáférést adni.

Ahhoz, hogy megadhassuk az LDAP-hoz tartozó beállításokat, a `config/authsources.php` fájlt kell szerkesztenünk. Az alábbi kódrészletet elegendő beszúrni, és az egyes változóknak a helyi LDAP-nak megfelelő adatokat értékül adni.

```
'example-ldap' => array(
    'ldap:LDAP',

    /* The hostname of the LDAP server. */
    'hostname' => 'ldap.example.org',

    /* Whether SSL/TLS should be used when contacting the LDAP server. */
    'enable_tls' => FALSE,

    /*
     * Which attributes should be retrieved from the LDAP server.
     * This can be an array of attribute names, or NULL, in which case
     * all attributes are fetched.
     */
    'attributes' => NULL,

    /*
     * The pattern which should be used to create the users DN given the username.
     * %username% in this pattern will be replaced with the users username.
     *
     * This option is not used if the search.enable option is set to TRUE.
    'dnpattern' => 'uid=%username%,ou=people,dc=example,dc=org',
```

```
     */

    /*
     * As an alternative to specifying a pattern for the users DN, it is possible to
     * search for the username in a set of attributes. This is enabled by this option.
     */
    'search.enable' => TRUE,

    /*
     * The DN which will be used as a base for the search.
     * This can be a single string, in which case only that DN is searched, or an
     * array of strings, in which case they will be searched in the order given.
     */
    'search.base' => 'ou=people,dc=example,dc=org',

    /*
     * The attribute(s) the username should match against.
     *
     * This is an array with one or more attribute names. Any of the attributes in
     * the array may match the value the username.
     */
    'search.attributes' => array('uid', 'mail'),

    /*
     * The username & password the simpleSAMLphp should bind to before searching. If
     * this is left as NULL, no bind will be performed before searching.
     */
    'search.username' => 'cn=simplesamlphp,dc=example,dc=org',
    'search.password' => 'servicepassword',

    'priv.read' => TRUE,
    // The DN & password the SimpleSAMLphp should bind to before
    // retrieving attributes. These options are required if
    // 'priv.read' is set to TRUE.
    'priv.username' => 'cn=simplesamlphp,dc=example,dc=org',
    'priv.password' => 'servicepassword;,
  ),
```

Metaadat alapok

A beállítandó IdP alapvető paraméterei a `metadata/saml20-idp-hosted.php` fájlban állíthatók. Az alábbi kódrészlet egy minimális, de már működő példát mutat.

```
$metadata['__DYNAMIC:1__'] = array(
    /*
     * The hostname for this IdP. This makes it possible to run multiple
     * IdPs from the same configuration. '__DEFAULT__' means that this one
     * should be used by default.
     */
    'host' => '__DEFAULT__',

    /*
     * The private key and certificate to use when signing responses.
     * These are stored in the cert-directory.
     */
    'privatekey' => 'saml-example-org.key',
    'certificate' => 'saml-example-org.crt',

    /*
     * The authentication source which should be used to authenticate the
     * user. This must match one of the entries in config/authsources.php.
     */
    'auth' => 'example-ldap',
);
```

Megfelelő beállítások után a dinamikusan generált metadata a `/saml2/idp/metadata.php` útvonalon érhető el.

Tesztelés

Legegyszerűbben a telepített SSP felületén tudjuk ellenőrizni, hogy a beállított autentikációs forrás működik-e. A felületen az Authentication fül alatt található egy 'Test authentication sources' link, amelyre kattintva látható minden beállított autentikációs forrás is, így a két alapértelmezett, teszt célokat szolgáló alatt a most beállított example-ldap névre hallgatónak is meg kell jelenni. (A közvetlen url erre az oldalra: simplesaml/module.php/core/authenticate.php) Ez utóbbira kattintva a beállított LDAP-ból autentikálva be kell tudnunk jelentkeznünk; siker esetén az LDAP-ból kinyerhető attribútumokat láthatjuk.

Service Provider (SP) beállítás

Alapbeállítások

A telepített alkalmazásunk által kezelt SP-ket a **config/authsources.php** fájlban tudjuk beállítani. Az *entityID, idp, discoURL* értékeket most hagyjuk *NULL* értéken és adjuk hozzá a **privatekey** / **certificate** részt.

A SimpleSAMLphp a tanúsítvány fájlokat a korábban létrehozott **cert** mappában fogja keresni, a fájlokat elég relatív elérési úttal megadni.

```
 'default-sp' => array(
        '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 should SP should contact.
        // Can be NULL/unset, in which case the user will be shown a list of available IdPs.
        'idp' => NULL,

        // The URL to the discovery service.
        // Can be NULL/unset, in which case a builtin discovery service will be used.
        'discoURL' => NULL,

        'privatekey' => 'saml-example-org.key',
        'certificate' => 'saml-example-org.crt',

 ),
```

A fenti beállítások alapján az SP entityID-ja megegyezik a metadata elérési útvonalával (szokásos megoldás SSP-nél), nem adunk meg alapértelmezett idp-t, ezáltal az SSP választási lehetőséget kínál fel számunkra, mikor az SP-re szeretnénk bejelentkezni, ill. most még Discovery Service URL-t sem adunk meg, hanem a beépítettet használjuk. Ez utóbbit majd a HREF-be történő integrációkor meg kell változtatni - lásd lejjebb.

Az SP készen áll arra, hogy összekössük egy IdP-vel (ez jellemzően szintén egy SimpleSAMLphp alkalmazás). Ehhez szükséges, hogy SP oldalon beállítsuk az IdP metadata-t és IdP oldalon is beállítsuk az SP metadata-t.

Metadata

Metadata fájlok

A különböző metadata template fájlok a **metadata-templates** mappában találhatóak. A nekünk szükséges template fájlt másoljuk át a metadata mappába.

- **SP** oldalon lennie kell egy **metadata/saml20-idp-remote.php** fájlnak. Ez a fájl tartalmazza az IdP eléréséhez szükséges adatokat.

```
cp metadata-templates/saml20-idp-remote.php metadata
```

- **IdP** oldalon lennie kell egy **metadata/saml20-sp-remote.php** fájlnak. Ez a fájl tartalmazza az SP eléréséhez szükséges adatokat.

```
cp metadata-templates/saml20-sp-remote.php metadata
```

Metadata letöltés

Ezen az oldalon megtaláljuk az SP vagy IdP-re vonatkozó **metadata**-t, **XML** és **PHP** formátumban:

https://example.org/simplesaml/module.php/saml/sp/metadata.php/default-sp?output=xhtml

SP metadata beállítás IdP oldalon

A metadata **simplesaml** kezdőlapon, az alábbi helyen érhető el:

- Magyar nyelv esetén: "Föderáció" fül / "SAML 2.0 SP Metaadatok" pont alatt a "Mutasd a metaadatokat" linkre kattintva juthatunk el a fenti menüponthoz.
- Angol nyelv esetén: "Federation" fül / "SAML 2.0 SP Metadata" pont alatt a "Show metadata" linkre kattintva juthatunk el a fenti menüponthoz.

A "*SimpleSAMLphp fájl formátumban - akkor használható, ha a másik oldalon SimpleSAMLphp van*" mezőből tegyük a vágólapra az alábbi PHP kódot:

```
$metadata['https://example.org/simplesaml/module.php/saml/sp/metadata.php/default-sp'] = array
(
  'SingleLogoutService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://example.org/simplesaml/module.php/saml/sp/saml2-
logout.php/default-sp',
    ),
  ),
  'AssertionConsumerService' =>
```

```
  array (
    0 =>
    array (
      'index' => 0,
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'https://example.org/simplesaml/module.php/saml/sp/saml2-acs.php/default-
sp',
    ),
    1 =>
    array (
      'index' => 1,
      'Binding' => 'urn:oasis:names:tc:SAML:1.0:profiles:browser-post',
      'Location' => 'https://example.org/simplesaml/module.php/saml/sp/saml1-acs.php/default-
sp',
    ),
    2 =>
    array (
      'index' => 2,
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact',
      'Location' => 'https://example.org/simplesaml/module.php/saml/sp/saml2-acs.php/default-
sp',
    ),
    3 =>
    array (
      'index' => 3,
      'Binding' => 'urn:oasis:names:tc:SAML:1.0:profiles:artifact-01',
      'Location' => 'https://example.org/simplesaml/module.php/saml/sp/saml1-acs.php/default-
sp/artifact',
    ),
  ),
  'contacts' =>
  array (
    0 =>
    array (
      'emailAddress' => 'admin@example.org',
      'contactType' => 'technical',
      'givenName' => 'Example Corp. IT Dept.',
    ),
  ),
  'certData' =>
```

```
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==',
);
```

A vágólapra másolt kódot IdP oldalon, a **metadata/saml20-sp-remote.php** fájl végére illesszük be.

IdP metadata beállítás SP oldalon

A metadata **simplesaml** kezdőlapon, az alábbi helyen érhető el:

- Magyar nyelv esetén: "Föderáció" fül / "SAML 2.0 IdP Metaadatok" pont alatt a "Mutasd a metaadatokat" linkre kattintva juthatunk el a fenti menüponthoz.
- Angol nyelv esetén: "Federation" fül / "SAML 2.0 IdP Metadata" pont alatt a "Show metadata" linkre kattintva juthatunk el a fenti menüponthoz.

A "*SimpleSAMLphp fájl formátumban - akkor használható, ha a másik oldalon SimpleSAMLphp van*" mezőből tegyük a vágólapra az alábbi PHP kódot:

```
$metadata['https://idp.example.org/simplesaml/saml2/idp/metadata.php'] = array (
  'metadata-set' => 'saml20-idp-remote',
  'entityid' => 'https://idp.example.org/simplesaml/saml2/idp/metadata.php',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp.example.org/simplesaml/saml2/idp/SSOService.php',
    ),
  ),
  'SingleLogoutService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp.example.org/simplesaml/saml2/idp/SingleLogoutService.php',
    ),
  ),
  'certData' => 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==',
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
);
```

A vágólapra másolt kódot SP oldalon, a **metadata/saml20-idp-remote.php** fájl végére illesszük be.

Tesztelés

A fent elvégzett alapbeállítások után már tudjuk tesztelni a, hogy a felépített IdP - SP kapcsolat működik-e.

SP oldalon nyissuk meg a **simplesaml** kezdőlapot:

- Magyar nyelv esetén: "Azonosítás (autentikáció)" fül / "Azonosítási (autentikációs) beállítások tesztelése" link / "default-sp" link-re kattintva tudjuk tesztelni az IdP - SP kapcsolatot.
- Angol nyelv esetén: "Authentication" fül / "Test configured authentication sources" link / "default-sp" link-re kattintva tudjuk tesztelni az IdP - SP kapcsolatot.

A legördülő menüben az IdP-nk "nevére" kattintva, be kell tudnunk jelentkezni (az IdP-n keresztül). Ha működik, akkor az IdP visszairányít az SP-re, kiírja az azonosított felhasználó attribútumait.

Az alapvető lépsekkel kész vagyunk, van egy működő SP-nk és egy működő IdP-nk.

HREF-integráció

Metadata beállítása (IdP és SP is)

Javasolt dinamikus metaadatforrást (MDX) használni, opcionálisan kiegészítve statikus állományokkal. Részletes leírás itt: SimpleSAMLMixedMetadata

IdP

Amennyiben van SSP alapú IdP-nk, melyet szeretnénk a föderáció részévé tenni, úgy a teendők a következők.

- (Az adminisztratív teendőktől itt most eltekintünk, a csatlakozás folyamata itt van leírva)
- Kell küldeni egy levelet a info@eduid.hu címre, benne néhány mondat mellett az IdP metaadatának URL-jével (https://example.org/simplesamlphp/saml2/idp/metadata.php)
- Ha minden rendben megy, akkor az IdP bekerül a Resource_Registry-be, ezáltal a föderációs metaadatba is.
- Az előző pontban leírt módon be kell állítani a központi metadata feldolgozását.
- Amennyiben a föderációs metaadatban már szerepel a mi IdP-nk is, úgy a föderáció valamelyik, tesztelési célokat szolgáló SP-jénél ki is próbálhatjuk a bejelentkezést.

- **Fontos**, hogy a föderációs Discovery Service óránként generálja újra az IdP-k listáját, így ennyi idő mindenképp szükséges, hogy az új IdP megjelenjen itt, az egyes SP-k pedig két óránként töltik újra a metaadatot, így előfordulhat, hogy azonnal nem fog minden működni, de néhány óra alatt várhatóan beindul. :)
- Tesztelésre használható oldal: https://attributes.eduid.hu
- Ahhoz, hogy a Resource Registry-be is be tudjunk lépni és az IdP további, a föderációra vonatkozó beállításait meg tudjuk ejteni, ehhez az IdP-nek ki kell adnia az alábbi attribútumokat:
  - mail - ez belépés után, manuálisan is beállítható
  - eduPersonPrincipalName
  - schacHomeOrganizationType (az attribútumot hamarosan kivezetjük a kötelező attribútumok közül)
  - eduPersonScopedAffiliation

Attribútumok kezelése

Beállított IdP-nk alapértelmezés szerint azokat az attribútumokat adja ki, melyeket a metaadat alapján az SP kért (Lásd a metadatában a RequestedAttribute elemeket), és egyúttal alapból meg tudta szerezni a felhasználói adatbázisból, esetünkben az LDAP-ból. Mivel néhány attribútum nem szerepel az LDAP-ban, hanem az IdP-ben kell előállítani, így pár helyen módosítanunk kell az alapértelmezett konfiguráción.

A `metadata/saml20-idp-hosted.php` fájlba szerkesszük be az alábbi kódrészlet értelemszerűen módosított változatát. Az `'auth' => 'example-ldap',` sor alatt kezdjük. Fontos, hogy egyúttal a config.php `authproc.idp` részét kikommentezzük, nehogy az ottani sorszámokkal megadott default feladatok bekavarjanak.

```
'AttributeNameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
 'userid.attribute' => 'uid', // Itt adjuk meg, hogy mely, az LDAPból származó attribútum
alapján fogja az IdP kiszámítani az eduPersonTargetedID-t
 'authproc' => array(
                10 => array(
                        'class' => 'core:AttributeMap',
                        'uid' => 'eduPersonPrincipalName'
                //Itt az 'uid' az az attribútum az LDAP-ban, amely a felhasználó azonosítóját
tartalmazza, mert ebből képezzük az eduPersonPrincipalName-t.
                ),
                # 20 => array(
                #         'class' => 'core:AttributeAdd',
                #         'schacHomeOrganizationType' =>
array('urn:schac:homeOrganizationType:hu:university')
                # //Kötelező statikus attribútum az
```

```
[[HREFAttributeSpec#schacHomeOrganizationType|intézmény jellegének]] megfelelően
                # ),
                30 => array(
                        'class' => 'core:AttributeAlter',
                        'subject' => 'eduPersonPrincipalName',
                        'pattern' => '/^.*$/',
                        'replacement' => '${0}@intezmenydomain.hu',
                // Itt adjuk hozzá az intézményi scope-ot az eduPersonPrincipalName már
meglévő értékéhez
                ),
                40 => array(
                        'class' => 'core:AttributeAlter',
                        'subject' => 'eduPersonAffiliation',
                        'pattern' => '/^.*$/',
                        'replacement' => '${0}@intezmenydomain.hu',
                // Itt adjuk hozzá az intézményi scope-ot az eduPersonAffiliation már meglévő
értékéhez
                ),
                50 => array(
                        'class' => 'core:AttributeMap',
                        'eduPersonAffiliation' => 'eduPersonScopedAffiliation'
                // Az LDAP-ból eduPersonAffiliation-ként érkező attribútumból föderációs
elvárásoknak megfelelően eduPersonScopedAffiliationt készítünk
                ),
                60 => array(
                        'class' => 'core:AttributeAdd',
                        'eduPersonScopedAffiliation' => array('member@intezmenydomain.hu')
                // Az eduPersonScopedAffiliation-ben tesztelés céljából kiadhatjuk member
értéket,
                // így ha LDAP-ból nem jön érték, akkor is láthatjuk, hogy működik az
attribútum kiadás
                ),
                61 => array(
                        'class' => 'core:TargetedID',
                        'nameId' => TRUE,
                ),
               // Itt állítjuk be, hogy az IdP előállítson és kiadhasson állandóazonosítóként
eduPersonTargetedID-t, ha kérik
                70 => array('class' => 'core:AttributeMap',
                        'name2oid'
```

```
                // Az LDAP-os attribútum nevekből itt kreálunk szabványos urn:oid
formátumúakat
                ),
                80 => 'core:AttributeLimit',
              ), // .authproc
       'simplesaml.nameidattribute' => 'eduPersonPrincipalName',
       'attributeencodings' => array(
               'urn:oid:1.3.6.1.4.1.5923.1.1.1.10' => 'raw',
        ),
        'sign.logout' => true
```

- További tudnivalók a Resource Registry-ről, ill. a Föderációs attribútum specifikációról.
- Ha minden rendben ment, akkor a Resource Registry-ben regisztrált IdP-hez tartozó adminisztrációs jogok átkerülnek az IdP technikai gazdájához, s ezzel a folyamat kész is.

SP

Amennyiben IdP-t is beállítottunk, és be is tudunk lépni a Resource Registry-be, úgy nincs más dolgunk, mint az RR-ben új SP-t hozzáadni a föderációhoz, amely a megfelelő átfutási idő után a föderáció minden tagjánál látható is lesz.

Ellenkező esetben (nincs IdP, és nem is tervezünk beállítani), akkor az IdP hozzáadásánál részletezett pontokon kell végig menni a metaadat betöltéséig, s a továbbiakat az említett e-mail címen megbeszélni.

Attribútum scopeok használata

A HREF föderáció IdP-i ún. scopeolt attribútumokat is használnak. Ez a scopeolás azt jelenti, hogy minden egyes IdP csak a saját scopejában ad ki attribútumokat, és a Shibboleth SP-k ezt ellenőrzik is. A scope és az attribútum valódi értéke egy '@' karakterrel kerül elválasztásra (ilyen attribútumok jelenleg: eduPersonScopedAffiliation illetve eduPersonPrincipalName).

A SimpleSAMLphp alapértelmezett telepítése nem szűri a hibásan scopeolt értékeket. Kiegészítő modulként szűrésre használható az NIIF által fejlesztett attributescope modul, ami reményeink szerint rövid távon a hivatalos SimpleSAMLphp kiadás része lehet.

A telepítésről és konfigurációról bővebben itt lehet olvasni: https://github.com/NIIF/simplesamlphp-module-attributescope

- Az `attributescope` modul használata esetén a következőképp kell módosítani a `config/config.php` fájlt:

```
authproc.sp =  array(
                     ...
                    // 49 => array('class' => 'core:AttributeMap', 'oid2name'),
                    50 => array(             'class' => 'attributescope:FilterAttributes'
                    ),
                    ...
                ),
```

Figyeljünk arra, hogy mire a modulhoz ér a vezérlés, az attribútumok nevei *friendlyName* alakúak legyenek (ne pedig *oid*-ok). A példában erre utal a 49-es sor.

Változat #1
document-uploader hozta létre 2025-08-07 12:03:48 CEST
document-uploader frissítette 2025-08-07 12:03:48 CEST