SSP EntityCategories

Ez a lap a simpleSAMLphp EntityCategories moduljának továbbfejlesztett változatához tartozó beállításokat ismerteti. Reményeink szerint a modul valamikor a simpleSAMLphp alapcsomagjának is része lesz, ám amíg ez nem történik meg, addig az alábbiak szerint érdemes eljárni, ha használni szeretnénk.

A modul forrása: https://github.com/sitya/simplesamlphp-module-entitycategories.git

Fontos, hogy a modul nem helyettesíti a core:AttributeLimit, vagy a niif:AttributeLimit modult, valamelyikkel együtt használandó!

Telepítés composeren keresztül

```
cd /path/to/simplesamlphp
composer require simplesamlphp/simplesamlphp-module-entitycategories:dev-master
composer config repositories.simplesamlphp/simplesamlphp-module-entitycategories vcs
https://github.com/sitya/simplesamlphp-module-entitycategories.git
composer update
```

Beállítás

Lévén egy AuthProc modullal van dolgunk, így a rendes authproc szekcióba kell elhelyeznünk valahol a sorban, a core:AttributeLimit, vagy niif:AttrobuteLimit előtt. Az alább részletezett alapbeállításokon túl (`default, strict, allowRequestedAttributes`) az egyes entityCategory-k URI-jait kell megadni, mint egy tömb kulcsát, és a hozzátartozó tömb értékeiként pedig a megengedett attribútumok URN-jeit. Tetszőleges számú entityCategory-t megadhatunk, a korábbi beállítások elsősorban azt szabályozzák, hogy mi történjen akkor, olyan entitással van dolgunk, akinek nincs a metadatájában megadva EntityCategory, vagy ha van, nem illeszkedik az általunk explicit beállított listában található EntityCategory-k valamelyikére.

Működő példa

```
75  => array(
        'class' => 'entitycategories:EntityCategory',
        'default' => true,
        'strict' => true,
        'allowRequestedAttributes' => true,
        'http://eduid.hu/category/registered-by-eduidhu' => array (),
        'http://www.geant.net/uri/dataprotection-code-of-conduct/v1' => array (),
        'http://refeds.org/category/research-and-scholarship' => array(
            '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
        ),
),

80 => array(
      'class' => 'niif:AttributeLimit',
      'default' => true,
      'bilateralSPs' => array(
          'google.com' => array('mail'),
          'urn:federation:MicrosoftOnline' => array('IDPEmail', 'ImmutableID'),
       ),
),
```

A fenti példa az alábbiakat végzi:

1. a magyar föderáció által regisztrált entitások számára a Resource Registry-ben beállított attribútumok (`RequestedAttributes`) alapján történik az attribútum kiadás;
2. a GÉANT Code of Conduct entitás kategóriájú eduGAIN-es SP-k számára szintén `RequestedAttributes` alapján történik az attribútum kiadás;
3. a Research & Scholarship entitás kategóriájú eduGAIN-es SP-k számára kiadjuk a kategória által igényelt attribútumcsomagot
   - az ilyen SP-k `RequestedAttributes` alapján módosíthatnak az attribútum igényeiken
4. a fenti kategóriáknak nem megfelelő SP-k közül kizárólag a *bilateralSPs* tömbben megadott entitásoknak adunk ki attribútumot.

> **Warning**

> Az *entitycategories:EntityCategory* modul *strict* beállítása esetén a lokálisan felvett SP-k esetén nem lesz figyelembe véve az *attributes* tömbelem! Ez azt jelenti, hogy a nem a központi metaadatokból származó SP-ket fel kell venni az *niif:AttributeLimit* modul listájába. Ebből fakadóan ilyen esetben nem is használhatjuk a *core:AttributeLimit* modult.

Opciók

`default`

Logikai kapcsoló, `true/false` értékeket vehet fel. Amennyiben `true`, úgy a beállított EntityCategory-k alatt megadott attribútumkészletet akkor is kiadjuk az adott EntityCategory-val érkező SP-nek, ha az attribútumokat explicit, a `RequestedAttribute`-ok között nem kérte felsorolva. Ennek az R&S EntityCategorynál van különös jelentősége (a példában is ez szerepel), mert ott a specifikáció kimondja, hogy a meghatározott attributúmkészletet akkor is ki kell adni az R&S-t támogató IdP-nek, amennyiben nincsenek ezen attribútumok tételesen felsorolva, mint `RequestedAttributes`.

`strict`

Logikai kapcsoló, `true/false` értékeket vehet fel. Amennyiben `true`, úgy csak és kizárólag a modul konfigurációjában megadott EntityCategory-val érkező SP-k számára kerülnek attribútumok kiadásra, "ismeretlen" EntityCategory-val bíró, és EntityCategory nélküli SP-k számára nem kerül kiadásra semmi.

`allowRequestedAttributes`

Logikai kapcsoló, `true/false` értékeket vehet fel. Amennyiben `true`, úgy megengedjük, hogy egy SP a hozzátartozó EntityCategory konfigurációjában megadott attribútumlistán túl kért attribútumot kiadásra `RequestedAttributes`-on keresztül, `false` esetén csak a listában szereplő attribútumok kiadását engedi a modul. Amennyiben az érték `true` és a `strict` értéke `false`, úgy az "ismeretlen" EntityCategory-val bíró SP-k számára is a `RequestedAttributes` alapján kerülnek kiadásra az attribútumok.

Változat #2
document-uploader hozta létre 2025-08-07 12:04:57 CEST
cziernorbert frissítette 2026-04-13 15:39:43 CEST