OpenSSO IdP - SimpleSAMLphp SAML2 SP

Cél

OpenSSO hosztolt IdP és SimpleSAMLphp SP összekapcsolása a SAML2 protokoll segítségével.

SimpleSAMLphp telepítése

[[http://rnd.feide.no/content/installing-simplesamlphp]]

Konfigurációs paraméterek (config/config.php)

A következő paramétereket érdemes beállítani kezdésképp:

```
secretsalt: egy titkos 32 bájtos véletlenszám, amit a titkosításhoz használni fog a simplesamlphp
technicalcontact_name,email: az üzemeltető technikai kapcsolattartója
logging_handler: file / syslog
debug: bekapcsolva minden saml kérés és válasz megjelenik a webes felületen (kényelmes!)
enable.saml20-sp, enable.saml20-idp, enable.shib13-sp, enable.shib13-idp
default-saml20-idp: Discovery Service megkerülése és fix IdP választása
```

IdP metaadat beállítása

metadata/saml20-idp-remote.php:

```
'https://idp.sch.bme.hu/niif-teszt' =>  array(
  'name'                                =>      'NIIF Test at idp.sch.bme.hu',
  'description'                   => 'Log in via idp.sch.bme.hu',
  'SingleSignOnService'   =>
'http://maszat.sch.bme.hu:58080/opensso/SSORedirect/metaAlias/niif-teszt/idp',
  'SingleLogoutService'   =>
'http://maszat.sch.bme.hu:58080/opensso/IDPSloRedirect/metaAlias/niif-teszt/idp',
  'base64attributes'              =>      false,
  'request.signing' => false,
  'certificate' => "maszat-idp.crt",
  'certFingerprint' => "DE:F1:8D:BE:D5:47:CD:F3:D5:2B:62:7F:41:63:7C:44:30:45:FE:33",
  'saml2.relaxvalidation' => array('noattributestatement')
)
```

A cert könyvtárba mentsük le a maszat-idp.crt-t (például a maszat idp metaadatból kimásolva).

A fenti konfiguráció HTTP/Redirect bindingot használ a SAML Requestre, a választ pedig HTTP/Post-on keresztül kapja. Fontos, hogy a base64attributes ki legyen kapcsolva, ugyanis az OpenSSO IdP nem kódolja base64-be az attribútumokat a SAML Response-ban.

SP metaadat beállítása

metadata/saml20-sp-hosted.php:

```
'https://maszat.sch.bme.hu/simplesamlphp/sp/niif-teszt' => array(
  'host'  => 'maszat.sch.bme.hu',
/*'privatekey' => 'server.pem',
  'certificate' => 'server.crt',
  'request.signing' => true,*/
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'
)
```

Ezután a /simplesamlphp/saml2/sp/metadata.php?output=xml URL-en keresztül tudjuk elérni az SP metaadatot. Fontos, hogy ebben a generált metaadatban nem tükröződik pl. a signing certificate és a NameIDFormat beállítás, ezért ezeket kézzel kell beleszerkeszteni.

Miután kijavítgattuk a metaadat fájlt, az OpenSSO adminfelület Federation -> Import Entity parancsával tudjuk importálni a megfelelő Realm-be. Importálás után a Circle of Trust

konfigurációhoz is hozzá kell adni a SimpleSAMLphp SP-t.

Problémák

Nincsenek :)

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:34 CEST
cziernorbert frissítette 2026-04-14 13:22:34 CEST