

SimpleSAMLphp_proxy_vidyo_portálhoz

Vidyo Portal Authentication Proxy

A vidyo portál utolsó fejlesztései lehetővé tették a SAML alapú autentikációt, és autorizációt.

Az implementáció nem teljesen fedi le a SAML feature-öket, az SP implementáció csak egy IdP-vel képes kapcsolatot létesíteni.

A portált a simpleSAMLphp proxy-ként való telepítésével tehetjük egy föderáció tagjává.

simpleSAMLphp telepítése

A simplesamlphp telepítését elvégezzük a [dokumentáció](#) szerint.

SSP IdP oldalának konfigurálása, illesztés a Vidyo portál felé

Legelőször is engedélyezni kell az IdP funkciót

config/config.php

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

Gyártsuk le az IdP certificate-jét, és rakjuk a cert könyvtárba *idp.pem*, illetve *idp.crt* néven.

```
cd cert
```

```
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out idp.crt -keyout idp.pem
```

metadata/saml20-idp-hosted.php

```
'auth' => 'default-sp',  
'privatekey' => 'idp.pem',  
'certificate' => 'idp.crt',  
)
```

A vidyo portál admin felületéről le kell tölteni a portál metaadatát, és el kell menteni a metadata könyvtárba.

metadata/vidyo-sp.xml

Erre hivatkozni kell a *config/config.php*-ben is:

```
'metadata.sources' => array(  
    ...  
    array('type' => 'xml', 'file' => 'metadata/vidyo-sp.xml'), // vidyo sp  
    ... ),
```

Vidyo admin portál

A portálon be kell állítani,

- hogy az azonosítás SAML alapú legyen, *Authentication Type*
- fel kell tölteni az IdP metaadatát, ezt az ssp telepítés *saml2/idp/metadata.php* oldaláról tölthetjük le. *Identity Provider (IdP) Metadata XML*
- be kell állítani az auto provisioninget, *SAML provision type*

Az előző fejezetben említett portál metaadatát ezen az oldalon érjük el. *View Service Provider (SP) metadata XML* Össze kell illeszteni a SAML rétegből jövő attribútumokat a Vidyo portál által használt adatmodellel. *Edit IdP Attribute Mapping...*

VidyoAdmin1.png

A *SAML IdP Attribute Name* oszlopokba az SSP-től kapott attribútum neveket kell írni. Ha a proxy IdP oldalán a példa szerint állítottuk be az *AttributeMap* szűrőt, akkor itt az attribútumok friendly nevét kell beírunk. Tipp:

<https://github.com/simplesamlphp/simplesamlphp/blob/master/attributemap/name2oid.php>

VidyoAdmin2.png

Bizonyos attribútumoknál lehetőség van érték mapping-re is, tipikusan csoport, vagy típus jellegű attribútumoknál, ahol a kapott attribútumok értéke alapján történik a megfeleltetés.

VidyoAdmin3.png

SSP SP oldalának konfigurálása, illesztés a föderációba

A proxy egyik oldala a föderáció felé, mint SP viselkedik. Az authsource-ot 'default-sp'-nek nevezzük el, erre kell hivatkozni a későbbiekben az IdP konfigurációban.

A *config/config.php* file-ba

Hogy a vidyo portál, és egyéb autentikációs szűrők futtatásakor az attribútum megfeleltetéseknél ne okozzanak gondot az oid formátumú attribútum nevek, mielőtt kiadjuk őket, az *AttributeMap* szűrő segítségével alakítsuk át az attribútum neveket.

config/config.php

```
'authproc.sp' => array(
    ...
    200 # > array('class' => 'core:AttributeMap', 'oid2name'),
    ...
),
```

Ha még nem tettük meg, rakjunk ide is certificate-et.

```
cd cert
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out sp.crt -keyout sp.pem
```

és könyveljük be a *config/authsources.php* -ba

```
'default-sp' => array(
    'saml:SP',
    ...
    'privatekey' => 'sp.pem',
    'certificate' => 'sp.crt',
    ...
)
```

metadata

Az SP-t regisztráljuk be a kívánt föderációba a föderáció által megadott szabályok alapján.

metarefresh

Hogy a metadatok mindig napra készek legyenek, gondoskodjunk a metarefresh és cron modul beállításáról.

A konfigurációs file-okat a config könyvtárba kell elhelyezni a sablonokat a modulok config-templates alkönyvtáraiban találjuk meg.

A modulok bekapcsolásáról a rendszer konfigurációban rendelkezhetünk a legegyszerűbben.

config/config.php

```
'module.enable' => array(  
    'cron' => TRUE,  
    'metarefresh' => TRUE,  
),
```

Változat #3

dziernorbert hozta létre 9 április 2025 16:35:13

dziernorbert frissítette 10 április 2025 09:53:19