MTA SZTAKI

Virtual Organizations,

intézményi csoportkezelés föderatív környezetben

Szabó Gyula
ITAK-TECH

2012. november 8.

Indítékok
A VO helye
A VO felépítése
Az alkalmazás
Képernyőképek
Gondolatok

Indítékok

Intézményünkben egyre több alkalmazást állítunk át AAI azonosításra. Megjelent az igény, hogy a SAML képes alkalmazások a névtár attribútumai alapján kezeljék a felhasználó jogosultságait.

Ez általában az osztály attribútumok alapján történt, de erről gyorsan kiderült, hogy kevés. Finomabb szabályozásra volt szükség. Kivételeket képezni és menedzselni roppant nehéz, ráadásul ezeket sok-sok alkalmazáson könyvelni kell.

Hová vezet mindez? Kifelejtett alkalmazások; ezt nem érem el - azt nem érem el; bentfelejtett felhasználók, akiknek már rég semmi közük az alkalmazásokhoz, jogaik mégis vannak.

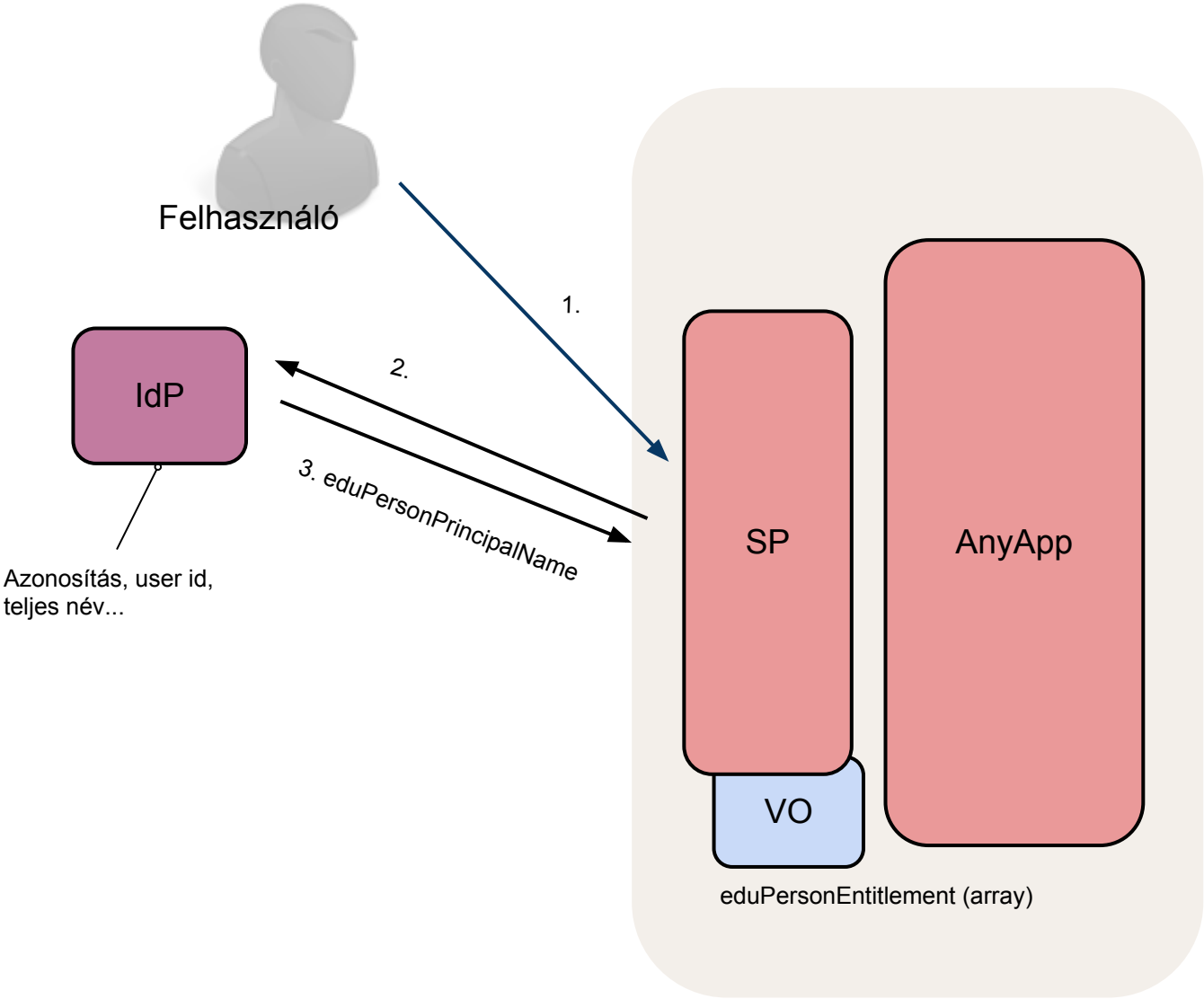
Olyan rendszer kell, amivel egy csoportot bárki - aki projekteket menedzsel - létrehozhat, és a szervezett csoportoknak az alkalmazásokhoz pár kattintással jogosultságokat lehet adni.

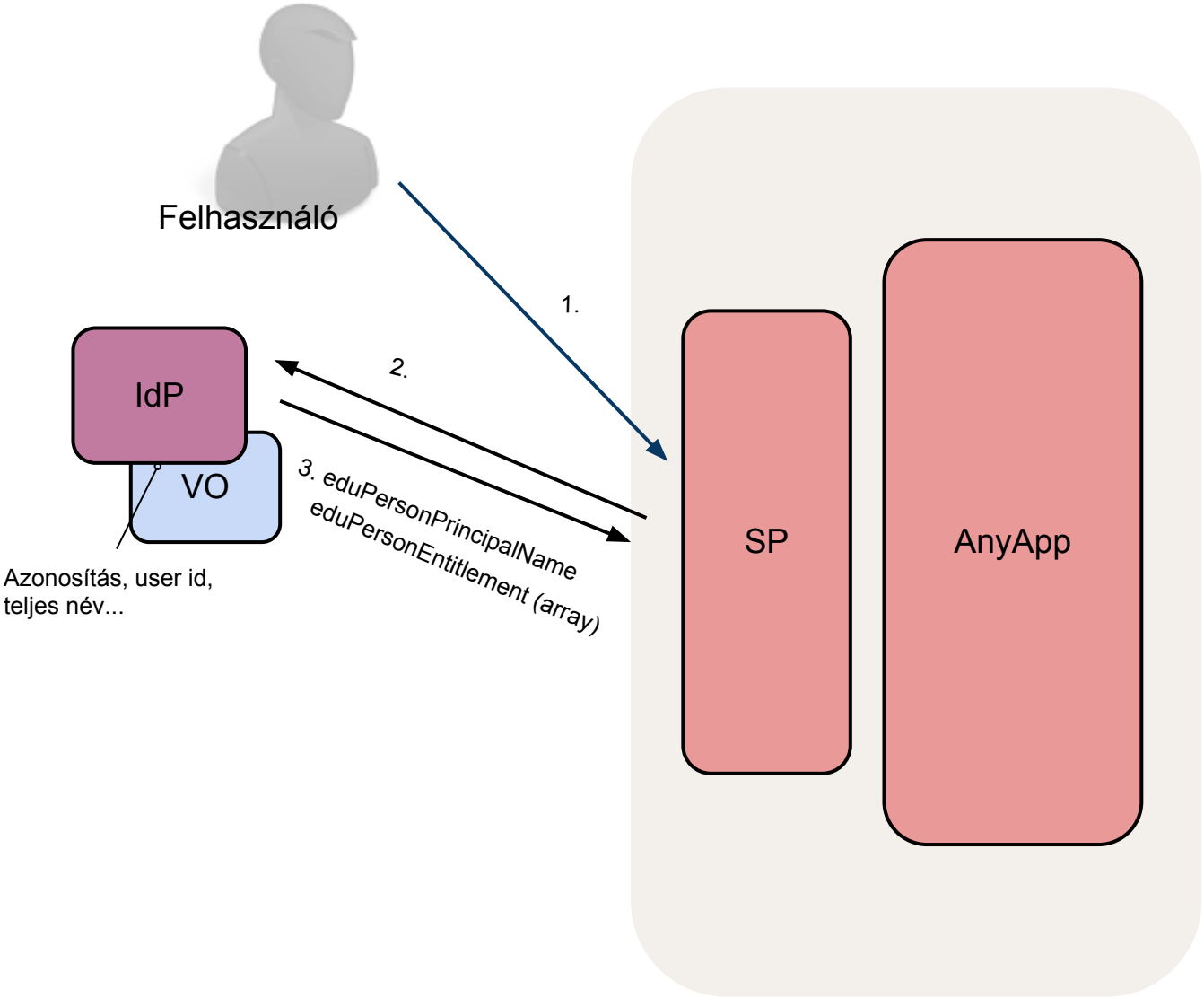
Ha valakit meghívunk a szervezetbe, akkor az egyből kapja meg az alkalmazásokhoz a megfelelő jogosultságokat, és "kiközösítése" esetén egycsapásra meg lehet vonni tőle az összes alkalmazáshoz adott jogosultságot.

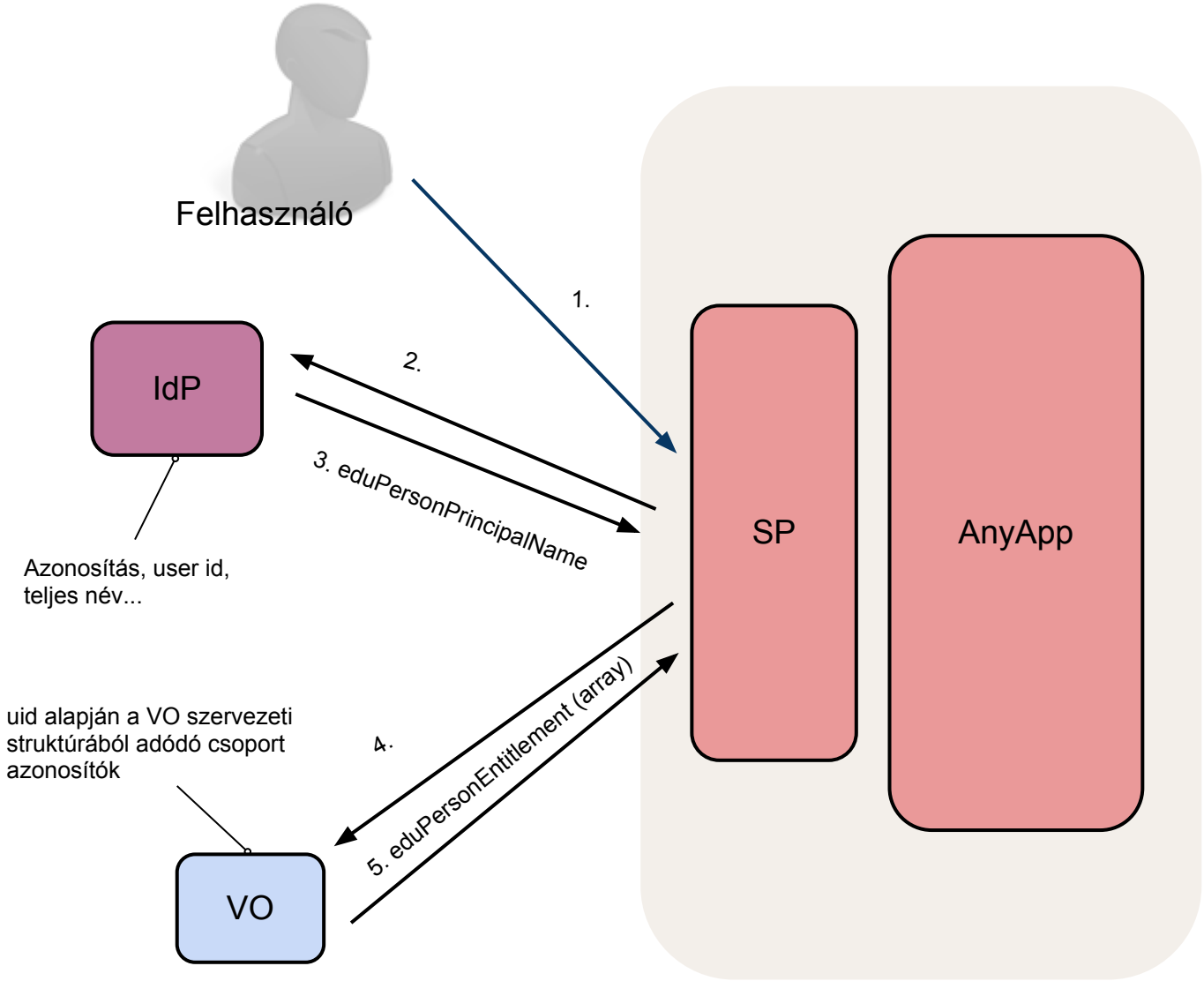
Legyen a neve, mondjuk: **VO***

* VO != VHO

A VO helye


Felhasználó
1.
2.
3. eduPersonPrincipalName
IdP
Azonosítás, user id,
teljes név...
SP
AnyApp
VO
eduPersonEntitlement (array)


Felhasználó
1.
2.
IdP
VO
3. eduPersonPrincipalName
eduPersonEntitlement (array)
Azonosítás, user id,
teljes név...
SP
AnyApp

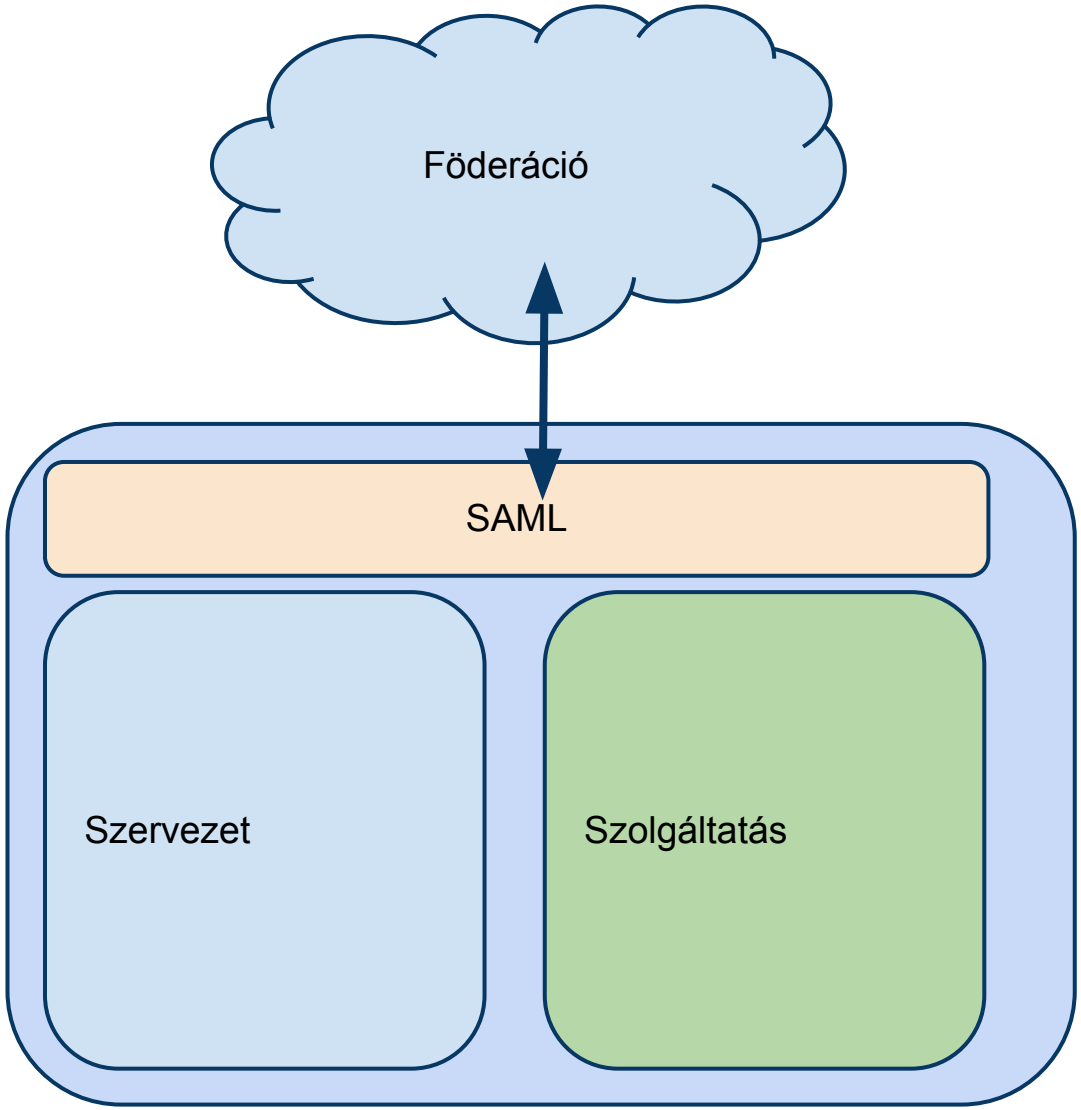

Felhasználó
1.
IdP
2.
3. eduPersonPrincipalName
SP
AnyApp
Azonosítás, user id,
teljes név...
uid alapján a VO szervezeti
struktúrából adódó csoport
azonosítók
4.
5. eduPersonEntitlement (array)
VO

A VO felépítése

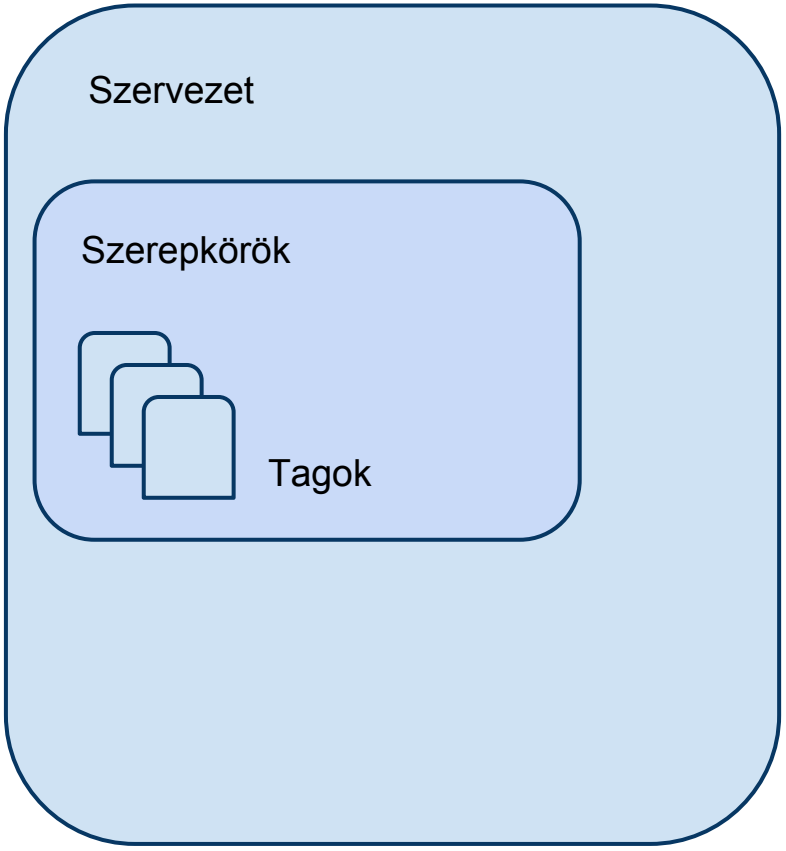
Kell egy szervezet menedzser

Kell egy szolgáltatás regiszter

Kell egy SAML interface



Szervezetek



Szervezet, bárki létrehozhat.

Szerepkörök, a valós szervezeti struktúrát képezze le.

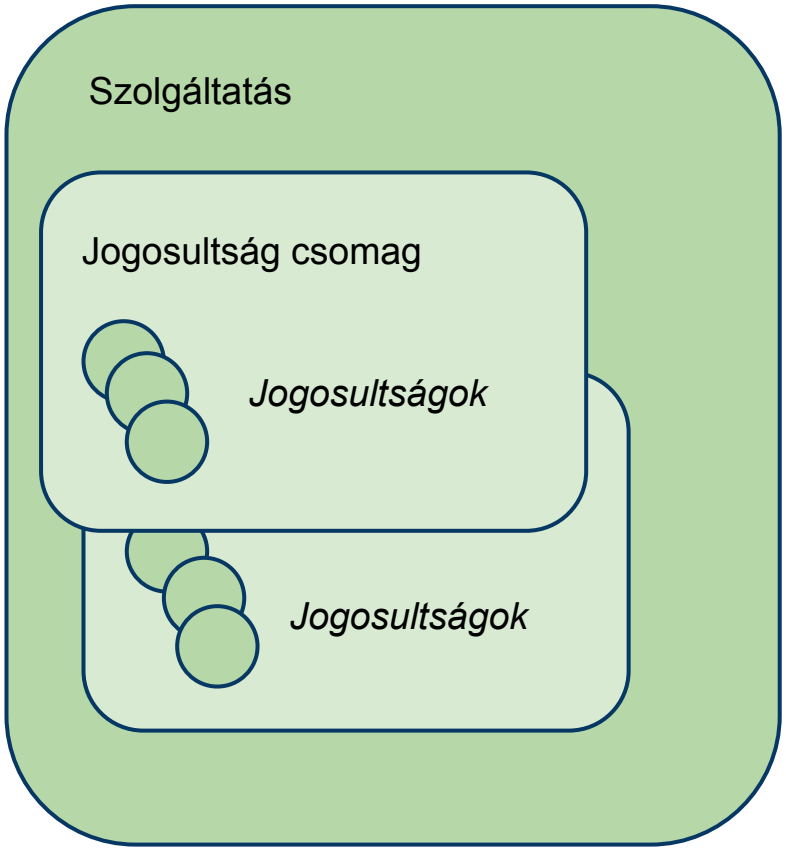
Tagok, meghívás útján kerülnek be, szerepkörökhöz rendelhetőek.

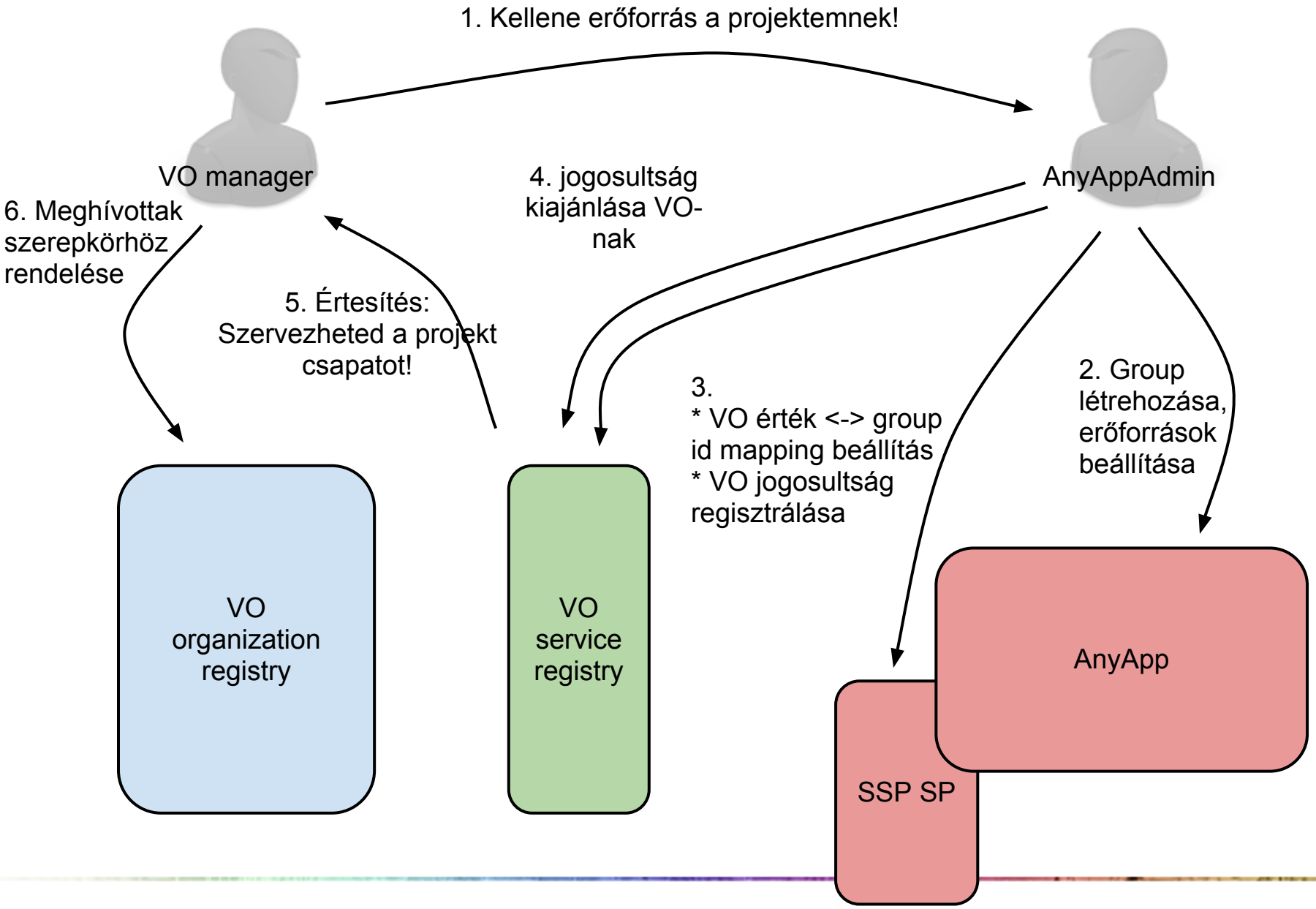
Szolgáltatás regiszter

Szolgáltatást be kell regisztrálni

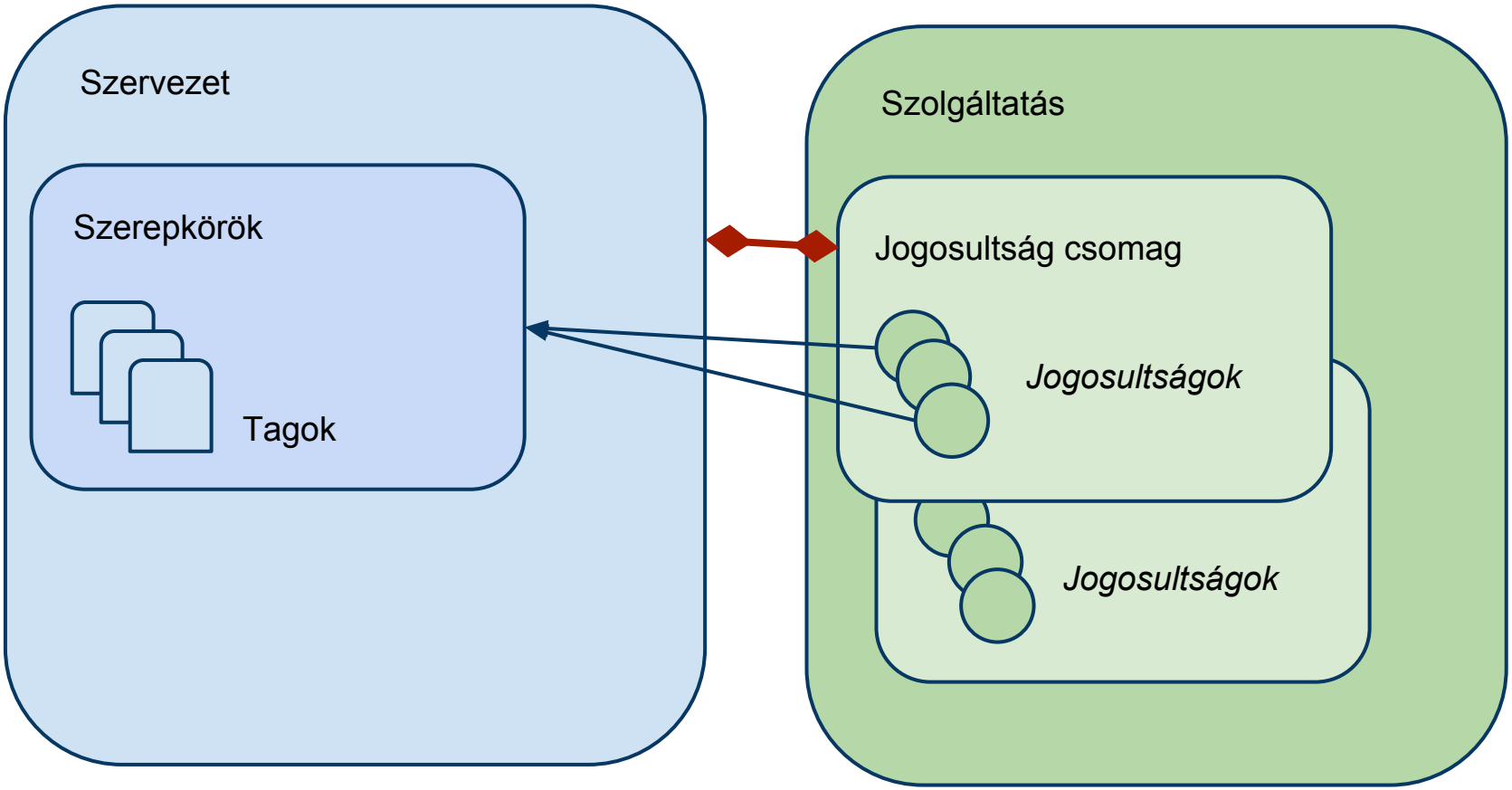
Jogosultságokat kell definiálni, összhangban az alkalmazás csoportjaival

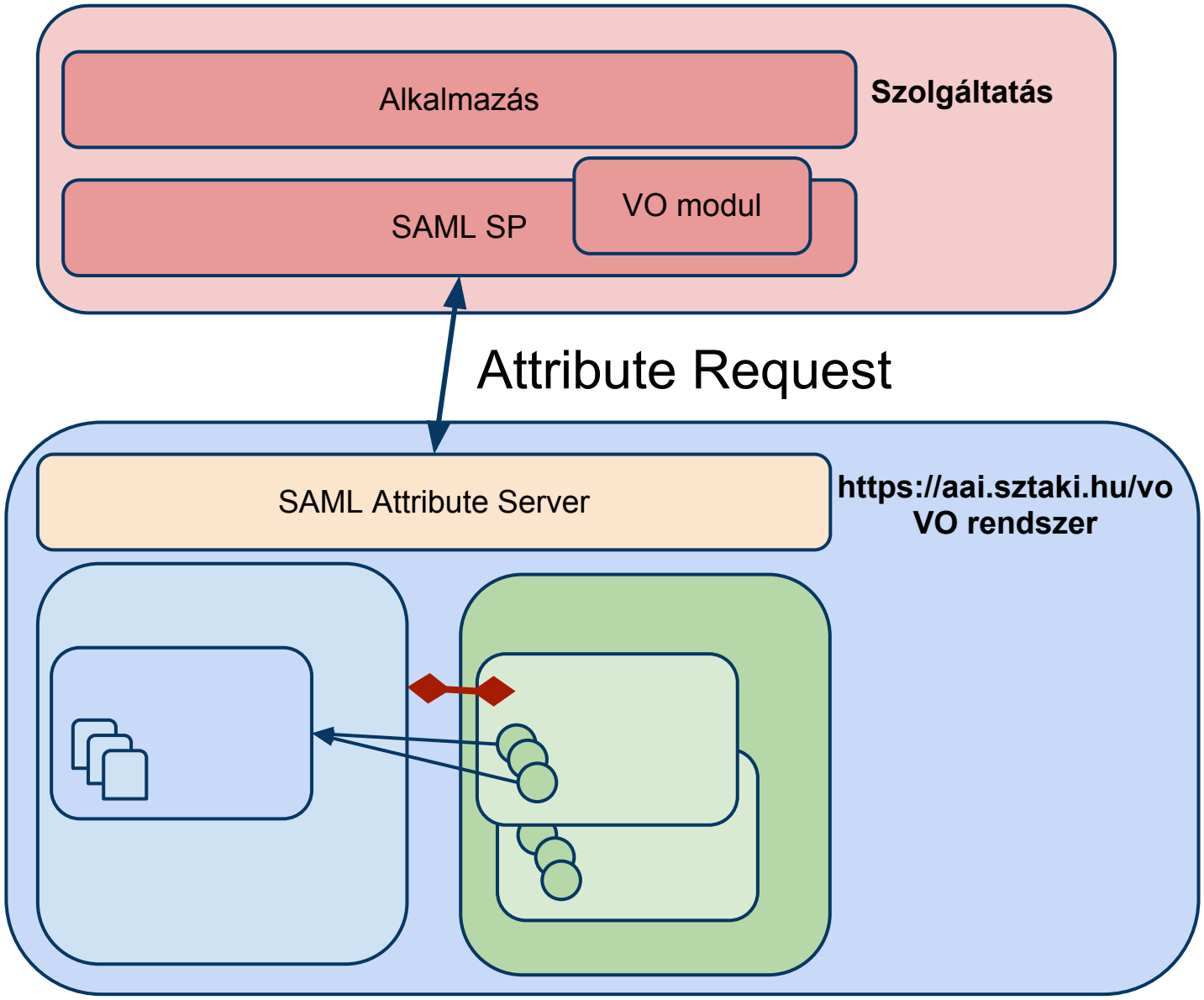
Jogosultság csomagokat kell összeállítani, amit egyes szervezeteknek ki lehet ajánlani

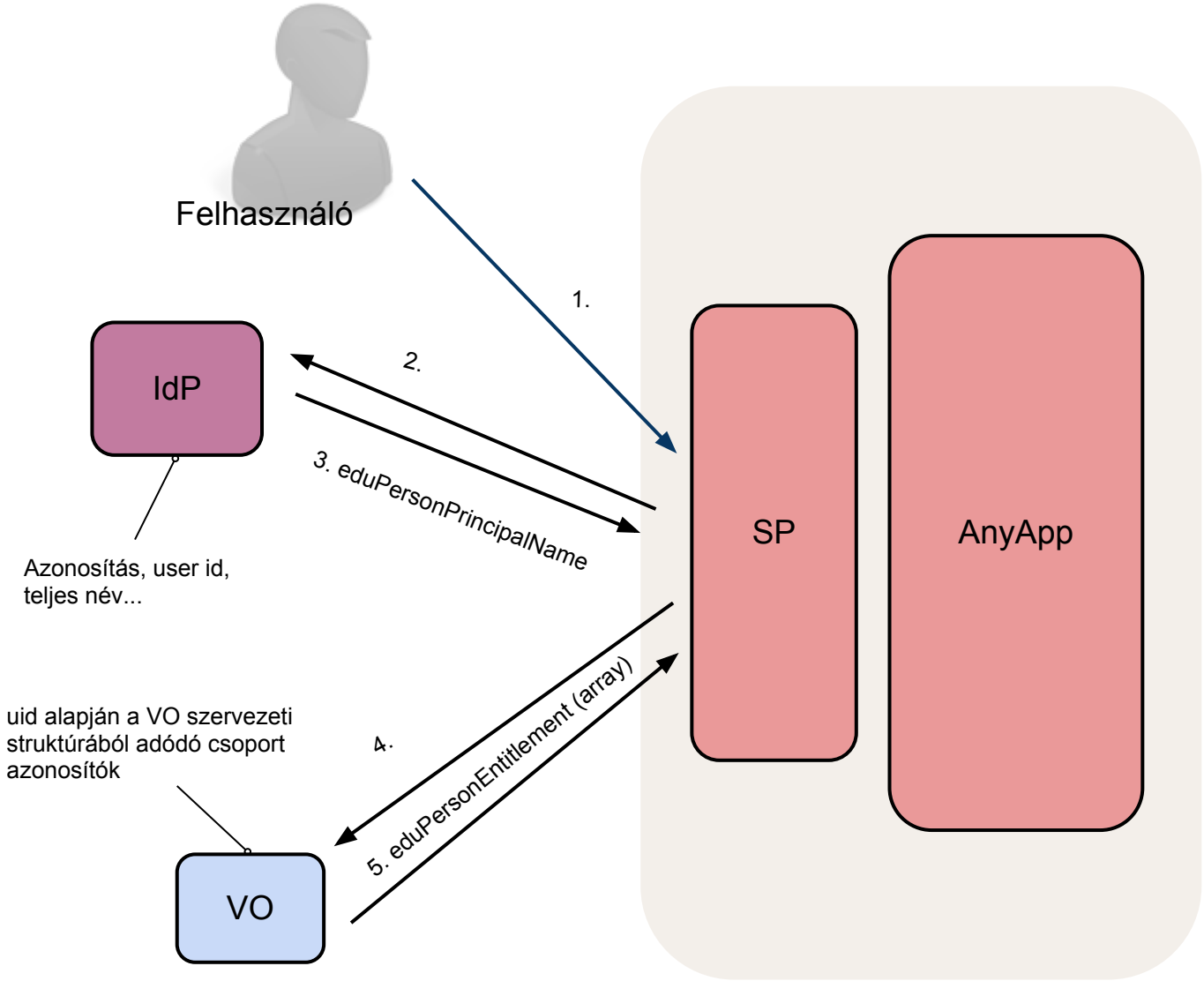



1. Kellene erőforrás a projektemnek!
VO manager
AnyAppAdmin
6. Meghívottak szerepkörhöz rendelése
4. jogosultság kiajánlása VO-nak
5. Értesítés: Szervezheted a projekt csapatot!
3.
* VO érték <-> group id mapping beállítás
* VO jogosultság regisztrálása
2. Group létrehozása, erőforrások beállítása
VO organization registry
VO service registry
AnyApp
SSP SP

Szervezet és szolgáltatás




Alkalmazás
Szolgáltatás
SAML SP
VO modul
Attribute Request
SAML Attribute Server
https://aai.sztaki.hu/vo
VO rendszer


Felhasználó
1.
IdP
2.
3. eduPersonPrincipalName
SP
AnyApp
Azonosítás, user id,
teljes név...
uid alapján a VO szervezeti
struktúrából adódó csoport
azonosítók
4.
5. eduPersonEntitlement (array)
VO

Az alkalmazás

Mielőtt regisztrálunk a VO-ba

Az alkalmazás gazdájának meg kell oldani, hogy az SP felől jövő csoport attribútum értékek összerendelődjenek az alkalmazás csoportjaival.

Ha a felhasználó még nem járt az alkalmazásnál, akkor létrehozza, felhasználva az IdP-től kapott személyes adatokat (név, email cím, preferált nyelv) (**create**)

A gyakorlat általában az, hogy ha nincs még ilyen csoport, akkor az auth logika létrehozza az új csoportot (**create**).

A felhasználót hozzárendeli a VO-tól származó csoportokhoz (**update**).

Az újabb szoftvereknél már egyre többször találkozunk moduláris authentikációs driverekkel (pl: opennebula, icinga). Érdemes megírni a SAML drivert, hamar behozza az árát.

MTA SZTAKI

SimpleSAMLphp modul konfiguráció

root@vh-frontend-1-G1:/var/simplesamlphp/config

```
        * Authentication processing filters that will be executed for all SPs
        * Both Shibboleth and SAML 2.0
        */
       'authproc.sp' => array(
            9 => array(
              'class' => 'vo:vo',
              'entityId' => 'https://aai.sztaki.hu/vo',
              'AAendpoint' => 'https://aai.sztaki.hu/vo/ssp/module.php/aa/attributeserver.php',
            ),
            10 => array(
                    'class' => 'core:AttributeMap', 'oid2name'
            ),
            61 => array(
                    'class' => 'authorize:Authorize',
                    'eduPersonEntitlement'    =>  array(
                              '/^urn:geant:niif.hu:sztaki:felho:.*/',
                     ),
            ),

            65 => array(
              'class' => 'attributeValueChooser:attributeValueChooser',
              'attributename' => 'eduPersonEntitlement',
              'mapping' => array(
                    'urn:geant:niif.hu:sztaki:felho:oneadmin' =>'oneadmin',
                    'urn:geant:niif.hu:sztaki:felho:users' => 'users',
                    ),
           ),
```

"config.php" 656L, 21068C written 422,65-72 67%

Képernyőképek

CloudADMIN

Frontend felhasználók ADMIN joggal

Szereplők
Ács Sándor
Szabó Gyula
Kotcauer Péter
Magyar Zsuzsanna
Héder Mihály
Gergely Márk
Marlok Tamás
Unicsovics Milán

Jogosultságok
frontend.felho.sztaki.hu::oneadmin

VO szervezet, szerepkörök

Frontend felhasználók USERS joggal

Frontend felhasználók USERS joggal

Szereplők
Ács Sándor
Szabó Gyula
Kotcauer Péter
Magyar Zsuzsanna
Héder Mihály
Gergely Márk
Marlok Tamás
Unicsovics Milán

Jogosultságok
frontend.felho.sztaki.hu::users

Projekt tag

Gondolatok

A szoftver

PHP, Symfony 1.4 keretrendszerrel
Élesben működik, a szolgáltatás regiszter alapja cserére szorul
Cloud szolgáltatásban szélesebb körben is gondoljuk nyújtani

simpleSAMLphp modulok:
aa - attribute authority server (Lantos Ádám exNIIF)
vo - modul az SP-hez
nincsenek publikálva.

Az alkalmazások

Teljes értékű alkalmazások, azonosításon kívül jogosultságkezelés is:

icinga, opennebula, ajaxplorer

Csak hozzáférés:

minden, amit simpleSAMLphp kiszolgál.

Az MTA SZTAKI intézményében egy új központi alkalmazás bevezetésénél feltett kérdés, a

tud-e SAML-ul?

már így hangzik:

tud-e VO támogatást?

A VO az MTA SZTAKI intézményén belül megállja a helyét, de egy decentralizáltabb struktúrákban,

- pl. **az újonnan összevont akadémiai kutatóintézeteknél**

-

hangsúlyosabban előjönnének a föderált azonosítási környezet és egy VO megoldás előnyei.

Kérdések

Köszönöm a figyelmet!