VO

Terminológia

- **Virtual Organization (VO)**: Felhasználókból álló csoport
- **VO Service**: Alkalmazás, melyet az egyes VO tagjai használnak
- **VO Service Group**: Alkalmazások egy csoportja, melyek egy közös entityID alatt kerülnek összefogásra, s melyek számára egy IdP ugyanazt a targetedID-t adja ki
- **VO Platform**: Az a szoftverkörnyezet, amely által lehetővé válik a VO tagok egyes VO Service-kbeli munkája.
- **VO Attributes**: Azok az attribútumok, melyek az adott felhasználó VO Platform-beli munkájához kapcsolódnak.
- **VO Management**: Felület, amelyen az felhasználók VO attribútumait lehet konfigurálni.
- **VO Attribute Authority**: Speciális IdP, melyet az egyes VO Service-k kérdeznek, ha egy-egy felhasználó VO Platform-beli attribútumára van szükségük.

Koncepció

Az alapprobléma

Az egyre inkább terebélyesedő föderációkban előbb-utóbb mindenhol előkerül a kérdés: miként lehet egyszerűen és hatékonyan megvalósítani egymástól független, különböző intézmények által azonosított felhasználók projektszintű együttműködését, tehát ad-hoc csoportok létrehozását? Mindezt úgy, hogy ez ne kívánjon speciális IdP/SP konfigurációt, .htaccess bütykölést, stb... hanem az egyes alkalmazások egy adott helyről be tudják szerezni a felhasználó az adott alkalmazáshoz kapcsolódó attribútumait.

Az ötlet

- Az egyes csoportokhoz tartozó felhasználók csoportmunkával kapcsolatos attribútumait gyűjtsük egy adatbázisba, tegyünk mellé egy webes felületet, így lehetőségünk lesz rá, hogy a felügyeletünk alatt álló csoportokat könnyen tudjuk adminisztrálni.
- Állítsunk üzembe egy IdP-t, amely autentikációt nem végez, kizárólag Attribute Authority szerepkörben dolgozik.

Tehát ha ehhez az IdP-hez fordul egy SP egy állandóazonosítóval, akkor az IdP az adott állandóazonosítóhoz tartozó attribútumokat kiadja számára, ezzel lehetővé téve, hogy az SP

ismerhesse, hogy az adott felhasználó milyen csoportokban milyen szerepeket tölt be, hogy az SP által védett alkalmazás ezek alapján állapíthassa meg a felhasználó alkalmazásszintű jogosultságait. Például: a felhasználó belép egy wiki alkalmazásba föderatív azonosítással, ekkor a felhasználót azonosító IdP-től az SP kap néhány attribútumot, ám azt - nyilvánvaló okokból - nem tárolja az IdP, hogy a felhasználó milyen ad-hoc csoportoknak tagjai, és ezeken a csoportokon belül milyen szerepkört tölt be, így az SP tovább kérdez, és ha a VO AA-tól megtudja, hogy a felhasználó tagja a wiki-adminisztrátorok csoportjának, akkor ezt az információt is tovább adja az alkalmazásnak valamilyen attribútum értékeként.

Az ötlet fenti két pontjának együttes megvalósítását nevezzük **VO Platformnak**. Egy felhasználó bármilyen ad-hoc csoportnak tagja lehet, így nem szükségszerű, hogy

--> folyt köv innen.

Ha az egyes VO-k által használt szolgáltatásokat (VO Service) egy csoportba rendezzük (VO Service Group), akkor lehetőségünk lesz a

Kérdések

Változat #1
document-uploader hozta létre 2025-08-07 12:05:12 CEST
document-uploader frissítette 2025-08-07 12:05:12 CEST