SAML protokoll alkalmazása nemzetközi kutatási programban

Uherkovich Péter
Pécsi Tudományegyetem
uherkovich.peter@pte.hu

Absztrakt

A Pécsi Tudományegyetem területén megkezdődött a SAML authentikációs protokoll bevezetése. Az intézményen belüli alkalmazások, valamint az országos szövetséghez való csatlakozás mellett megjelent a nemzetközi kutatási együttműködés támogatásának igénye is.

Társadalmi Megújulás Operatív Program 4.2.2.C-11/1/KONV-2012-0005 Jól-lét az információs társadalomban pályázat keretében egy pécsi kutatócsoport munkája kapcsolódik az „International Network of Territorial Intelligence" nemzetközi együttműködéshez. A kutatócsoport munkájából egy részterületet szeretnék kiemelni, mely a nemzetközi kutatói együttműködés authentikációs bázisának megteremtésére szolgál.

Webes szolgáltatások a PTE-n

A PTE-n régóta igény van a web alkalmazások központi névtárból történő authentikációjára. Korábban több különböző megoldást alkalmaztunk:

1. Központi névtár adatainak rendszeres importja
2. LDAP protokoll használata
3. egy saját fejlesztésű megoldás

A felsorolt megoldások mindegyike rendelkezett néhány hátránnyal:

- Nem naprakész (1)
- Nincs SSO
- Nem szabványos
- Nincs vagy kevés attributum adható át

SAML bevezetése

Az EDUID kapcsán bevezetett SAML protokoll megoldást nyújt a fenti problémákra. Bár a SAML protokoll kétoldali implementációja bonyolultabb, mint a korábban használatosak, az EduID miatt már létrehozott IdP-vel a feladat nagyobb részét elvégeztük, a SP oldali telepítés könnyebb.

Jelenleg még csak a PHP-s környezettel van tapasztalatunk, mert csak a SimpleSAMLphp megoldást próbáltuk. Külön könnyebbség, hogy pl. a Drupal keretrendszer tartalmaz kész simpleSAMLphp modult, valamint a linux disztribúciókhoz is elérhető a simpleSAMLphp modul.

A belső fejlesztők számára készült egy dokumentáció az SP telepítéséhez és a PTE IdP-hez történő csatlakoztatáshoz. A központi informatikai szervezeten kívül már két karon is használatba került a rendszer.

Az egyetemen belüli alkalmazások jellemzően a belső felhasználói kör számára készülnek, ezért ezeket az SP-ket nem csatlakoztattuk az EduID-hez. A technológia azonban már adott, így tehát amint igény mutatkozik a felhasználói kör kiszélesítésére, ez néhány adminisztratív lépéssel elvégezhető. Az EduID-hez nem csatlakoztatott alkalmazások esetében értelemszerűen nem használunk discovery service-t, ehelyett közvetlenül a PTE IdP-t hívjuk meg. Annak érdekében, hogy ez a belépési mód az EduID-tól megkülönböztethető legyen, bevezettünk a PTEid fogalmát, valamint az ehhez tartozó login ikont. Ennek működése csak a discovery hiánya tekintetében különbözik az EduID-től.

Az egyetemi működésben használt, azonosítást igénylő alkalmazásaink között nem nagyon látjuk azt a kört, amely igazán széles körű, intézményen kívüli felhasználóazonosítást tudna használni. Néhány közhasznú alkalmazás, mint például a filesender, vagy az NIIF központi, több intézmény számára nyújtott szolgáltatásának kezelőfelülete jó példa, azonban újabb ilyen alkalmazások az intézményünknél jellemzően nem születnek.

Az intézményközi együttműködés egyik területe a kutatási projektek lehetnek.

Nemzetközi kutatási projekt

Az „International Network of Territorial Intelligence” kutatói közösségben 10 európai és néhány tengerentúli ország különféle fajta kutatóintézményeinek dolgozói végeznek interdiszciplináris kutatást az élhető környezet és társadalom témaköreit érintő projektekben.

Az INTI kutatói hálózatban közel 40 intézmény közel 400 kutatója vesz részt. Az INTI különféle különálló kutatások zajlanak, melyek valamilyen szállal kapcsolódnak az anyaprojekthez. Az egyes kutatások és kutatók egymás közötti kapcsolatának erősítésére jött létre az INTIsc („International Network of Territorial Intelligence Service Cloud”) projekt, melynek célja technikai támogatást nyújtani a tágabb kutatói kör résztvevői számára.

A kutatói közösség már ma több közös kutatást támogató rendszert, adatbázist és honlapot használ, melyeken a széles körű hozzáférés igénye felmerült.

Annak érdekében, hogy az INTIsc központi alkalmazásba, valamint az egyes kutatási eredményekhez és kutatási eszközökhöz tartozó alkalmazásokba egységes beléptető platformot biztosítsunk, hoztuk létre az INTIsc keretein belül a központi authentikációs környezetet.

Megoldási lehetőségek

Az első elképzelés LDAP protokoll alkalmazása volt, majd miután a PTE-n bevezetésre került a SAML , ennek alkalmazása ígéretesebbnek tűnt. A SAML-lal kapc solatos korlátozott tapasztalat és illesztési lehetőségek miatt azonban olyan megoldást terveztünk, amely a háttérben az LDAP lehetőségét is tartalmazza.

A SAML alkalmazásával kapcsolatban további kérdésként merül fel, hogy milyen együttműködési köröket alakítunk ki.

A következő lehetőségeket vettük számba:

a) Önálló, független névtár és IdP kialakítása
b) Pont-pont bizalmi kapcsolatok kiépítése az érintett intézményekkel

c) Projekthez tartozó bizalmi szövetség kialakítása, melyhez az érintett anyaintézmények IdP-ikkel csatlakozhatnak
d) Projekt IdP és SP-k csatlakoztatása nemzeti szövetségekhez
e) Projekt IdP és SP-k csatlakoztatása nemzetközi szövetséghez

A fenti lehetőségek a SAML lehetőségei és filozófiája miatt természetesen nem zárják ki egymást.

A döntést nehezíti, hogy az érintett kutatói körnek vannak olyan tagjai, akiknek nincs SAML képes anyaintézményük. Az ő kiszolgálásuk érdekében mindenképpen meg kell valósítani az (a) megoldást, mely egyben az LDAP hátteret is biztosítja, ezért ebbe minden felhasználónk belekerül. Ez a megoldás az úgynevezett Virtual Home Organization.

Megoldandó kérdés az olyan attributumok kezelése, melyhez szükséges adatok kizárólag az INTIsc adatbázisából nyerhetők ki, például az INTIsc rendszerbeli csoport-hovatartozás. Rendszerünkben ez a kutatási projekthez vagy kutatócsoporthoz tartozást jelenti, mely információ ebben a formában nem áll más rendszerben rendelkezésre, hiszen egy kutatócsoportban vagy kutatási projektben akár különböző országbéli kutatók is részt vehetnek.

Ezért kiegészítésképpen tervezünk egy webszervizt, melynek a célja az egyes partner-alkalmazásoknak olyan információkat adni a felhasználókról, melyek a partner-IdP-ktől attributumban nem kapható meg. Ugyanakkor ennek a problémának a megoldására más, SAML szövetségi rendszerbeli megoldása is körvonalazódik másik projekt (HEXAA) kapcsán, annak eredményeit is felhasználhatjuk.

A projekt helyzete

A projekt megvalósítása jelenleg az (a) és (b) pontnál tart.

Készült egy SQL adatbázis, webes karbantartó felület és olyan LDAP szerviz, amely az SQL-beli adatokkal működik. Meghatároztuk az LDAP attributum sémát.

Meghatároztuk a SAML attributum sémát. Készült egy IdP, mely az LDAP-n keresztül kapja az adatokat. Ez a furcsa megoldás azt biztosítja, hogy a két technológiai vonal garantáltan ugyanazokat ez adatokat biztosítja.

Az INTIsc keretében tehát megvalósítottunk egy névtár adatbázist, mely a kutatási hálózat résztvevőinek teljes körét tartalmazza. Amíg a szövetségi authentikációs hálózat a részt vevő intézményekkel közösen kialakításra nem kerül, addig azonosítási bázisként ezt a névtárat használhatják a résztvevő kutatók.

Az INTIsc IdP-je tehát a központi névtárra támaszkodó SAML2 protokollt ismerő szabványos IdP. Technikailag a SimpleSAMLphp termék alkalmazásával valósítjuk meg, mely a Linux disztribúció részeként van telepítve.

Készült egy SP, mely technológiai mintaként szolgál további alkalmazások bekapcsoláshoz, egyben a rendszer adminisztratív kezelőfelületét biztosítja.

Készült egy dokumentáció az eddigiekről.

További tervek

A projekt további céljai egy központi kommunikációs és projektnyilvántartási rendszer, mely egyben technológiai minta is további szolgáltatások bekapcsolásához.

A rendszer fokozatos bevezetése és adatokkal történő feltöltése után tervezzük a további bizalmi kapcsolatok kiépítését folytatni.

Jelen állapotban is már jól látható, hogy egy ilyen rendszer megvalósításának fő nehézsége nem technológiai, hanem szervezési és bevezetési feladat.

Hivatkozások

- Simplesamlphp: http://simplesamlphp.org/
- EduGAIN: http://www.geant.net/service/eduGAIN/Pages/home.aspx
- PTE IdP: http://idp.pte.hu/
- INTIsc: http://intisc.org, http://idp.intisc.org
- HEXAA: http://www.terena.org/activities/tf-emc2/meetings/26/hexaa-emc2-201402.pdf