Resource Registry

> **Elavult információ**
>
> **Figyelem:** ez a szócikk elavult, a Resource Registry megújult egy ideje!

Alapfogalmak

- **Attribútum**: felhasználóra vonatkozó tulajdonság. A föderációban használt attribútumok listája **itt érhető el**.
- **SP: Service Provider - Szogáltatás**: Webes alkalmazás, amelynek felhasználóit föderatívan valamilyen IdP által autentikáltatja
- **IdP: Identity Provider - Azonosító szervezet**: Feladata a felhasználó azonosítása, felhasználó attribútumainak kiadása SP-k részére
- **Föderáció**: olyan intézmények halmaza, amelyek között lehetséges az azonosítási-információk átadása. Az intézmények - szabályozott keretek között - megbíznak a másik intézmény által kiállított azonosítási-információkban.
- **Entitás**: föderációt alkotó elem (IdP, SP)

Áttekintés

A Resource Registry az alakuló magyarországi felsőoktatási és kutatási föderáció (HREF) központi eleme, mellyel a föderációban résztvevő szolgáltatások (SP-k) és azonosító szervezetek (IdP-k) adminisztrálását lehet egy letisztult környezetben, elosztott jogosultságokkal végezni. A rendszer az egyes entitásokért felelős adminisztrátorok számára készül.

A rendszer a svájci SWITCH Intézet által fejlesztett rendszer alapjaira épül, PHP nyelven íródott, adatbázisként MySQL-t használ.

Funkciók

A rendszer saját adatbázisból dolgozik, minden funkciójának kimenete ezeken az adatokon alapul.

- Föderáció-szintű feladata, hogy a központi metaadatot óránként generálja, melyet a résztvevő "entitások" használnak, ezzel garantálva egyfelől a föderáció egységességét, másfelől a megfelelő formátumú metaadat alkalmazásával megteremtse a lehetőséget, hogy a föderáció kiegészítő alkalmazásai (Discovery Service), ill. nemzetközi szintű együttműködésben - bizonyos keretek közt - más föderációk is dolgozhassanak ebből.

- Az attribútum-szabályzat szintén föderációs szinten állítható, melyeket kiegészítve, az egyes IdP-k megadhatják, hogy mely attribútumokat milyen feltételekkel adják ki, ill. az egyes SP-k is deklarálhatják, hogy milyen attribútumok megléte esetén tudnak egyáltalán működni, mindezt az egyes intézmények adatvédelmi felelősei által kontrolálva.
- Egyénileg, az adott entitás adminisztrátorai által használhatók az egyes IdP-k, SP-k telepítését és konfigurálását megkönnyítő funkciók, melyek a megfelelő beállításokat webes felületen megadva letölthetővé teszik az ezen beállítások alapján automatikusan generált, és jó eséllyel minimális további kézi konfigurációt igénylő fájlokat. Fontos, hogy ezeket a fájlokat nem kötelező használni, ám segítséget jelenthetnek.

Shibboleth 2.x SP-hez:

- `shibboleth2.xml`

Fontos, hogy ezt akkor lehet szinte egy az egyben használni, amennyiben az adott SP csak egy alkalmazást véd. Amennyiben több alkalmazás is igényel Shibbolethet egyazon hoszton, úgy kézzel kell szerkeszteni az xml-t.

- `attribute-map.xml`
- `attribure-policy.xml`

Ez a két fájl egy az egyben használható letöltés után, további konfigurációt alapesetben nem igényel.

Shibboleth 2.x IdP-hez:

- `attribute-resolver.xml`

Ez csak egy keret fájl, a legtöbb olyan elem szerepel benne, amelyeket a helyi viszonyokra szabva már működhet az IdP, ám itt muszáj kézzel is szerkeszteni, pl. LDAP adatok...

- `attribure-filter.xml`

A fájl egyből használható - további információk a fájl előállításának menetéről.

SimpleSamlPHP-hoz:

- `AttributeFilter.xml`

A fájl egyből használható - további információk a fájl előállításának menetéről.

Bejelentkezés a rendszerbe

A Resource Registry a https://rr.eduid.hu címen érhető el, és bejelentkezni csak föderatív azonosítás után lehet. A nyitóképernyőn a bejelentkezési lehetőségen túl mindössze általános,

nyilvános információk érhetők el a föderáció aktuális állapotával kapcsolatban, ill. a rendszer használatához található segítség.

A rendszerbe történő bejelentkezéshez elengedhetetlen, hogy a felhasználót azonosító IdP az alábbi attribútumokat átadja a Resource Registry-nek.

- eduPersonPrincipalName
- schacHomeOrganizationType
- eduPersonScopedAffiliation
- email - ez belépés után, manuálisan is beállítható

Szerepek a rendszerben

A Resource Registrybe csak föderatív azonosítás után lehet belépni.

Felhasználó

- Lehetősége van rá, hogy a föderációhoz szolgáltatást (SP-t) regisztráljon, amely jóváhagyás után élesedhet.

SP adminisztrátor

- Ő felelős egy, vagy több, már jóváhagyott SP-ért, ill. elbírálhat felhasználói SP ajánlásokat.

IdP adminisztrátor

- Az általa regisztrált és karbantartott IdP-ért felelős.

RR adminisztrátor

- A Resource Registry-n belül tevékenykedő felhasználók jogosultságaiért felelős, ő adhat hozzá egyes entitásokhoz újabb adminisztrátorokat, ill. bírálhat el IdP-ket, és SP-ket.

Alapértelmezés szerint, aki be tud lépni, a legegyszerűbb felhasználói jogosultságokat kapja, bármilyen magasabb szintű szerepkört RR adminisztrátor delegálhat számára, a magasabb jogkörrel járó felelősségi kört pontosan körülhatárolva. (Pl. A RR adminsiztrátor a felhasználót az őt azonosító IdP adminisztrátorává tehet, amely nyomán a felhasználó pontosan ezt az egy IdP-t hangolhatja, de felhasználói jogosultságokat már nem oszthat tovább)

Fontos, hogy az RR-ben az egyes szerepek egy-egy intézmény adminisztrálásához köthetők, ily módon megvalósítva az elosztott jogosultságkezelést. Egy példán keresztül bemutatva ez azt jelenti, hogy egy felhasználó ha szeretne SP-t felvenni a föderációba, akkor azt csak az őt azonosító intézmény hatókörébe teheti meg, ami azt is jelenti, hogy az adott intézményhez tartozó, RR adminisztrátor jogosultsággal rendelkező felhasználó hagyhatja ezt a regisztrációs-, vagy módosítási kérelmet jóvá. Ugyanez az adminisztrátor csak a saját intézményéhez tartozó

entitásokra vonatkozóan oszthat, vagy vonhat vissza jogosultságokat.

Természetesen létezik Power User, aki mindent lát, mindenhez van jogosultsága, de csak nem várt esemény esetén aktivizálódik valahol az NIIF AAI környékén :), amúgy rendeltetésszerű működés esetén a szubszidiaritás elvét képviselve az intézményeké az őket érintő ügyekben a döntési jog.

Folyamatok

SP regisztráció

Bárki, akit a rendszer föderatív azonosítással beléptetett, kezdeményezheti egy SP föderációba történő felvételét, ehhez az „SP adminisztráció“ oldalon az „Új SP regisztrálása“ c. menüpontot kell választani. Varázsló segít a regisztrációban, melynek mindössze a telepített SP metaadatának nyilvánosan elérhető url-jét kell megadni (alapértelmezés szerint: https://#HOSTNAME#/Shibboleth.sso/Metadata), majd az automata a lehető legtöbb beállítási paramétert megpróbálja kiolvasni az xml-ből, és egyből beírni az adatbázisba az új SP adatai közé. Mivel minden adatot nem lehetséges az alapértelmezett metaadatból kinyerni, így a regisztráló felhasználónak néhány további adatot kell megadnia ahhoz, hogy véglegesíthesse az SP regisztrációs kérelmet. Ezeket hat csoportra lehet osztani.

- **Alapinformációk**: itt kerülnek megadásra az alapvető, leíró információk, melyek az SP nevét, leírását tartalmazzák, ill. a legfontosabb azonosító, az entityID. Az adatok egy része (pl: entityID) kiderül már a metaadatból is, így a beviteli mezőt már az automata kitöltötte.
- Itt tudjuk meghatározni első körben azt is, hogy az adott SP nyilvános, vagy belső SP legyen. Ennek szellemében kell a megadott feltételes mezőket kitöltenünk. Ha belső SP, akkor csak a legszükségesebb adatok megadása elvárt.
- **Kapcsolattartók**: ha a metaadatból nem derül ki, akkor kézzel kell megadni technikai, adminisztratív, általános...stb. kapcsolattartó személyeket, akik adatai a központi metaadatban is szerepelni fognak.
- **SP Service Locations**: különböző bindingok elérhetőségei – ezt az automata az esetek nagy hányadában jól kiolvassa a metaadatból, emberi módosítást a legritkább esetben igényel. Kivételt képez a *NameIdFormat* meghatározása, mely kapcsán három opció közül választhatunk.
  - Tranziens opciót kell választanunk, ha SP-nk számára nem fontos, hogy ki a felhasználó, hiszen nem ez alapján dől el, hogy milyen erőforrásokat érhet el, hanem az alapján hogy milyen, a felhasználóra vonatkozó, pl. eduPersonScopedAffiliation attribútumot állnak az SP rendelkezésére.
  - Perzisztens opciót kell választanunk, ha SP-nk számára fontos, hogy ki a felhasználó ÉS sz SP által védett alkalmazásaink is felkészültek arra, hogy persistent-idt fogadjanak, ezzel dolgozzanak.
  - Nem meghatározott opciót kell választanunk, amennyiben az SP által védendő alkalmazás mind persistent, mind transient NameID fogadására alkalmas.

- *Megjegyzés* Amennyiben most alakítjuk ki az AAI infrastruktúránkat, újonnan állítjuk be az SP-t annak érdekében, hogy valamilyen alkalmazást védjen, akkor *ajánlott*, hogy támogassa a perzisztens azonosítók használatát.
- **Tanúsítványok**: az SP által használt tanúsítványokat kell PEM formátumban megadni – ehhez is segítséget nyújt varázsló helyben, amelynek az SP metadatájának URL-jét címét kell megadni, ami után az automata beolvassa a tanúsítvány(oka)t.
- **Kötelező attribútumok**: itt lehetséges azon attribútumok megadása, melyek kiadása elvárt az IdP-től, amelyek nélkül az SP által védett alkalmazás nem használható.
- Amennyiben egy attribútumot megkövetel az SP használatához, az azt jelenti, hogy az attribútum kiadása nélkül az SP nem lesz használható. Ha egy attribútumot ajánlottnak jelöl, akkor az IdP kiadja, amennyiben implementálta, ám az SP-nek e nélkül is működnie kell. Ha olyan attribútumot jelöl kötelezőnek, amely a föderációs szabály szerint csak ajánlott, vagy opcionális, úgy könnyen előfordulhat, hogy az IdP nem implementálta, így nem is tudja kiadni, aminek következtében a felhasználó nem fogha tudni használni az Ön SP-jét.
- Ideális esetben nincs szükség külön szabályzásra, amennyiben mégis, úgy törekedjen rá, hogy minél kevesebb attribútumot szabályozzon külön!
- **Hallgatóság**: megadhatók, milyen jellegű IdP-k érhetik el az adott SP-t, ill. amennyiben ez a szabályzás nem lenne elegendő, úgy egyesével is megadhatók IdP-k aszerint, hogy felhasználói használhatják-e az SP-t, vagy sem.
- Amennyiben belső SP-t regisztráltunk, itt állíthatjuk be, hogy minden intézmény jelleget tiltunk, és egy kivételt megadunk: a saját IdP-nket. Ily módon más IdP nem is fog tudni erről az SP-ről, tehát annak ellenére, hogy szerepel a föderációs metaadatban, csak belső használatra lesz alkalmas.

SP módosítás

Egy jóváhagyott SP-t csak a megfelelő jogosultsággal rendelkező felhasználó tud módosítani. Általában egy-egy SP-hez tartozó adminisztrációs jogot az intézmény *RR adminisztrátor* jogkörrel rendelkező felhasználója osztja ki az adott SP jóváhagyásával egy ütemben.

A módosítás folyamata teljesen analóg a regisztrációéval, ami a funkciókat illeti.

FONTOS: Akár regisztráltunk, akár módosítottunk, a változásokat jóvá kell hagynia az Önt azonosító intézet RR adminisztrátorai közül valakinek. Amíg ezek a változtatások bekerülnek a föderációs metaadatba, az legfejjebb egy óra, ám amíg minden föderációs entitás frissíti a metaadatot, így értesül a változásról.

IdP regisztráció

A föderációba új IdP-t - mivel a regisztrálandó IdP-t üzemeltető kolléga még nem tud belépni a Resource Registry-be - egy, a föderációs adminisztrációért felelős kolléga tud regisztrálni. Ehhez szükséges, hogy az IdP, minden kapcsolódó programmal együtt telepítve legyen, és az alapértelmezett, telepítéskor generált metaadat egy meghatározott url-en elérhető legyen.

A telepítéshez - *Shibboleth esetében* - pl. a Shib2IdpInstall wikilapon található leírás szolgál segítségül. Attribútumokat, autentikációt konfigurálni nem kell, elegendő, ha a Teszt pontnál látjuk a megnyugtató `ok` szöveget, és minimális beállításokat megejtettük

Amennyiben ez működik, úgy írni kell egy e-mailt az aai@niif.hu címre, valaki a föderációs adminisztrátorok közül regisztrálja az IdP-t, és a válasz e-mailben elküld két linket, amelyek tartalmaznak két linket az `attribute-resolver.xml` és `attribute-filter.xml` már testreszabott konfigurációs fájlokra mutatva. Ezeket letöltve, bemásolva az IdP-nek már működnie kell alapszinten, így már lehetségessé válik a Resource Registry-be történő belépés. Sikeres belépés után az intézményhez tartozó RR jogosultságokat átadjuk, s a továbbiakban mehet minden a maga utáján, intézményi szinten.

Nagyon fontos, hogy az IdP-n bármilyen módosítás **azonnal érvénybe lép**, így rossz beállítás esetén akár az IdP által hitelesíthető felhasználók belépése is ellehetetlenülhet.

A beállítási lehetőségek az alábbiak

- **Alapinformációk**: IdP neve, leírása, jellege – technikai ismereteket nem igénylő, leíró jellegű információk
- **Technikai információk**: EntityID, és különböző bindingok elérhetőségei – ezt az automata az esetek nagy hányadában jól kiolvassa a metaadatból, emberi módosítást a legritkább esetben igényel.
- **Tanúsítványok**: az IdP által használt tanúsítványokat kell PEM formátumban megadni – ehhez is segítséget nyújt varázsló helyben, amelynek a webszerver címét kell megadni, ami után az automata beolvassa a tanúsítvány(oka)t.
- **Kapcsolattartók**: ha a metaadatból nem derül ki, akkor kézzel kell megadni technikai, adminisztratív, általános...stb. kapcsolattartó személyeket, akik adatai a központi metaadatban is szerepelni fognak.

A további négy beállítás némi hozzáértést igényel, lévén az alapértelmezett metaadatból nem olvashatók ki. A rendszer ezeket az értékeket a föderációs szabályoknak, megállapodásoknak megfelelően készíti elő, legtöbb esetben nincs szükség módosításra, ám ha mégis, bármilyen speciális igény okán, akkor nagy odafigyeléssel kell beállítani.

- **Támogatott attribútumok**: beállítandó, hogy az IdP mely attribútumokat, milyen formában támogatja. A föderációs szinten kötelezőket mindenképp támogatnia kell.
- **Általános attribútum kiadási szabályok**: beállítható, hogy amennyiben egy SP az adott attribútumot kötelezően, ill. opcionálisan kiadandóként kéri, akkor az IdP hogyan viselkedjen. Ezek a szabályok általánosak, minden, a föderációban résztvevő SP-r vonatkoznak.
- **Speciális attribútum kiadási szabályok**: beállíthatók külön-külön egyes SP-kkel való viselkedés, amennyiben indokolt az általános szabályoktól való eltérés.
- **Telepítési és környezeti információk**: leíró információk, amelyek pl. hiba esetén segítséget adnak a hiba elhárítójának, hogy milyen rendszerrel lesz dolga. Emellett statisztikai célokat is szolgál.

Attribútumok kezelése

A föderációban használható attribútumok részletes listája a föderációs attribútum specifikációban található.

Az egyes attribútumokkal kapcsolatban négy irányból lehetséges beállításokat eszközölni

- Minden SP meghatározhatja, hogy mely attribútumok kiadását követeli meg, és melyek kiadását ajánlja (SP beállítások - Kötelező attribútumok menüpont)
- Minden SP meghatározhatja, hogy mely IdP-ktől hajlandó attribútumokat elfogadni (SP beállítások - Hallgatóság menüpont)
- Minden IdP meghatározhatja általánosságban, hogy ha egy SP tőle egy bizonyos attribútum kiadását megköveteli, vagy ajánlja, akkor azt az attribútumot kiadja-e, vagy sem. (IdP beállítások - Általános attribútum kiadási szabályok menüpont)
- Minden IdP meghatározhat SP-specifikus szabályokat, tehát egy-egy SP-re, vagy egy-egy SP egy-egy attribútumára vonatkozólag megadhat az általános beállításaitól eltérő szabályokat - pl. az eduPersonPrincipalName-t ha általában ajánlva kérik az SP-k, akkor kiadja, de XY SP-nek semmiképp nem adja ki. (IdP beállítások - Egyedi attribútum kiadási szabályok menüpont)

További információ az attribútumok implementációjáról, kapcsolódó fogalmakról **A fenti beállítások eredőjeként generálódik az IdP-k által használandó XML alapú attirbútum filter fájl**

A generált attribútum filter alapvetően tiltó jellegű, tehát az IdP pontosan azokat az attribútumokat és pontosan azoknak az SP-knek adhatja ki, melyek megadásra kerültek a beállításoknál, egyébként semmit.

Néhány példa a "leképződésre"

- Ha egy SP kiadásra ajánl egy attribútumot, de az IdP (akár az általános-, akár az egyedi attribútum kiadási szabálya miatt) nem adja ki azt, akkor az XML fájlban komment formájában jelenik meg, hogy ezt és ezt az attribútumot igényelné az SP, de nem kerül kiadásra
- Ha egy SP hallgatóságából kitilt egy IdP-t, akkor az IdP attribútum filterében az adott SP-re vonatkozólag nem jelenik meg semmi, amelynek következtében nem is kerül számára kiadásra semmi

XML alapú filter

- Shibboleth IdP-nél: `attribute-filter.xml`
- simpleSAMLphp IdP-nél: `AttributeFilter.xml`

A filter fájlok Resource Registry által előállított változatát használni nem kötelező, de fokozottan ajánlott, hiszen ezzel garantálható egyfelől, hogy az IdP-n keresztül autentikáló felhasználók azokat az SP-ket, melyeket el kell tudniuk érni, jól fogják, megfelelő attribútumokkal "a zsebükben" fogják tudni elérni, másfelől így tudnak érvényesülni a feljebb részletezett korlátozó szabályzások.

Adatvédelmi szempontok

Ha egy SP megváltoztatja attribútum igényeit pozitív irányba (új attribútumokat kér), úgy a változtatás csak akkor fog belekerülni az IdP-k attirbútum filterébe, amennyiben ezt a változtatást tudomásul veszi az IdP oldaláról az illetékes adatvédelmi felelős. Amennyiben egy SP-nél ilyen jellegű változás történik, a rendszer e-mailben értesíti az érintett IdP-k gazdáit, adatvédelmi felelőseit.

Gyakorlati ajánlás

Kihasználandó a Resource Registry által biztosított lehetőségeket ajánljuk, hogy az IdP-hez tartozó generált attribútum filter fájlt automatikusan töltsék le az IdP-k, bizonyos időközönként (óránként, naponta párszor...), hiszen ezekbe csak úgy kerülhet változtatás, ha azt az IdP adatvédelmi felelőse jóváhagyta, akkor viszont egyből átvezetődik a változtatás, nem szükséges kézzel letölteni, ill. újraindítani az IdP-t. (Shibboleth esetében be kell állítani egy kapcsolót, SSP-nél automatikusan újratölti a friss XML-t)

A filter elérhetősége

- Shibboleth IdP: https://rr.eduid.hu/gen_attribute-filter.php/href/IDP_NEVE/attribute-filter.xml
- simpleSAMLphp IdP: https://rr.eduid.hu/gen_attribute-filter-ssp.php/href/IDP_NEVE/attribute-filter.xml

Útmutató a beállításhoz

- Shibboleth
- simpleSAMLphp

Változat #2
document-uploader hozta létre 2025-08-07 12:04:54 CEST
cziernorbert frissítette 2026-04-13 15:39:06 CEST