Attribútum specifikáció

Verzió: 2.0

(2017. november30.)

aai@niif.hu

E dokumentum célja

Egy SAML föderációban a felhasználóval kapcsolatos információkat az Identity Provider SAML Attribútumok formájában adja át a Service Provider számára. Fontos, hogy mindkét fél ugyanúgy értelmezze az adatokat.

Az attribútumok pontos meghatározását a vonatkozó séma dokumentumok tartalmazzák. Ebben a dokumentumban az alábbi sémákat használjuk:

- *person, organizationPerson* (X.521)
- *inetOrgPerson* (RFC2798)
- *eduPerson* (http://middleware.internet2.edu/eduperson/)
- *SCHAC* (https://wiki.refeds.org/display/STAN/SCHAC+Releases)
- *niifPerson, niifEduPerson* (NIIFSchema)

Ez az attribútum specifikáció a meghatározott attribútumok eduID föderációban belüli értelmezését adja meg. Bizonyos esetekben az értelmezés valamelyest kötöttebb, mint az eredeti meghatározás, annak érdekében, hogy a tartalomszolgáltatók pontosabb vagy használhatóbb információt kaphassanak.

A dokumentum kizárólag az eduID.hu föderáció által regisztrált entitásokra vonatkozik. Más föderációkból (pl. az eduGAIN-en keresztül elérhető) entitások esetén az ebben a dokumentumban szereplő – a sémáktól eltérő – megkötések nem érvényesek, azokat feltételezni nem szabad.

Az itt felsoroltakon túl az IdP-k tetszőleges attribútumot megvalósíthatnak és kiadhatnak bilaterális megállapodás alapján.

Attribútumok használata

Meghatározások

- **Implementáció** (megvalósítás): egy IdP abban az esetben *implementál* egy attribútumot, ha az attribútumban hordozott információ a föderációs specifikációnak megfelelő szemantikai és formai követelmények szerint a rendelkezésére áll. Egy implementált attribútum kiadása az IdP részéről csupán házirend kérdése.
- **Attribútum kiadás**: egy attribútum akkor kerül kiadásra, ha az adatot az IdP elküldi az SP számára. Nem minden implementált attribútum kerül kiadásra, kizárólag azok, amelyek az SP számára relevánsak.

Implementációs szintek

- **Kötelező**: az IdP-nek kötelező az attribútumot implementálnia.
- **Ajánlott**: javasolt minden IdP számára, hogy implementálja az attribútumot, azonban ez néhány intézménynél lehetetlen vagy nehézségekbe ütközhet.
- **Opcionális**: az IdP szabadon dönthet arról, hogy megvalósítja-e az attribútumot, azonban az implementációnak jelen specifikáció szerint kell történnie.

SP attribútum-igények

Az SP-k a Resource Registry-ben, és ezen keresztül a metadata állományban jelezhetik, hogy egy attribútum számukra megkövetelt (required) vagy opcionális.

- **Megkövetelt**: az alkalmazás működéséhez elengedhetetlen az attribútum, vagy az attribútum hiánya felhasználó számára jelentős akadályt vagy nehézséget jelent.

  pl. `eduPersonPrincipalName` olyan alkalmazásokhoz, amelyek nincsenek felkészítve átlátszatlan (opaque) azonosítók kezelésére

- **Opcionális**: az alkalmazás működését megkönnyíti az attribútum

  pl. a `displayName` attribútum átadásakor felhasználónak nem szükséges a teljes nevét az alkalmazáson belül megadnia.

Attribútumok listája

Összefoglalás

Kötelező attribútumok

eduPersonPrincipalName

eduPersonTargetedID

eduPersonScopedAffiliation

Ajánlott attribútumok

displayName

sn

givenName

mail

eduPersonEntitlement

Opcionális attribútumok

Az opcionális attribútumok közül csak azokat tartalmazza ez a dokumentum, amelyek esetében vagy a meghatározó sémához képest további megkötéseket tartalmaz, vagy az attribútumok elterjedtsége ezt indokolja.

cn

schacHomeOrganizationType

niifEduPersonAttendedCourse

niifEduPersonArchivedCourse

niifEduPersonHeldCourse

Állandó felhasználói azonosítók

Bizonyos alkalmazások esetén szükséges alkalmazás-specifikus adatokat is tárolni. Ilyen példa lehet egy webes naptárnál a felhasználóhoz kötődő bejegyzések, vagy egy wikinél a felhasználó szerkesztései. Ezeket az alkalmazások valamilyen helyi adatbázisban tárolják, a kulcs a felhasználó és az adatbázis bejegyzés között pedig egy **állandó azonosító**.

Az állandó azonosítók lehetnek:

- **statikusak**: a felhasználó létrehozásakor megadott adattal megegyezők
- **számítottak**: a felhasználó valamelyik (vagy több) attribútumából algoritmikusan - általában hash eljárással - generáltak
- **tároltak**: ezek általában olyan azonosítók, amelyet az IdP egy adatbázisban elsődleges kulcsként használ, azaz
    - a felhasználói attribútumok változása esetén is állandó marad
    - egyediségük biztosított

Az azonosítók az alábbi tulajdonságokkal rendelkezhetnek:

- **állandóság**: az IdP-nek gondoskodnia kell arról, hogy a kiosztott azonosító a felhasználó intézménynél töltött életciklusa során állandó legyen.

Amennyiben egy állandó(nak szánt) azonosító mégis megváltozik, az nagyon nehéz helyzetbe hozhatja mind a felhasználót, mind az alkalmazás üzemeltetőt.

- **nem osztható ki újra** (*non-reassignable*): az IdP-nek gondoskodnia kell arról, hogy egy felhasználó azonosítóját később nem osztja ki másik felhasználónak.

Ennek algoritmikus biztosítása bizonyos esetekben nehézségekbe ütközhet (pl. hash ütközések, illetve bizonyos IdP-k kézzel osztanak azonosítókat), ezért jelen specifikáció csak azt követeli meg, hogy azonosító a gyakorlatban ne tegye lehetővé, hogy az alkalmazás oldalán a felhasználók összekeveredjenek. Különböző IdP-ktől jövő felhasználók azonosítói abban az esetben nem ütközhetnek, ha az azonosítónak része valamilyen, az IdP-re jellemző adat (scope vagy entityID).

- **nem átlátszó** (*opaque*): az ilyen azonosítók nem jellemzők a felhasználóra, az értékéből nem lehet következtetni a felhasználó személyére (pl. e-mail címére)

Nem minden azonosító rendelkezik ilyen tulajdonsággal, azonban intézmények között adatvédelmi szempontból kifejezetten kívánatos, hogy egy azonosító ne legyen jellemző a felhasználó személyére. A nem átlátszó azonosítót nem célszerű a felhasználók felé megjeleníteni.

- **célzott** (*targeted*): az ilyen azonosítók minden SP-nél különbözőek, s így az SP-k - az IdP közreműködése nélkül - nem képesek profilt készíteni egy felhasználóról, ami adatvédelmi szempontból kívánatos.

Nem minden azonosító rendelkezik ilyen tulajdonsággal.

Az állandó azonosító kiadható attribútumként, illetve a SAML Assertion NameID mezőjében. Bizonyos SP implementációk (pl. a Shibboleth 2.x) képesek arra, hogy az alkalmazás részére elfedjék azt, hogy az azonosító pontosan milyen attribútumban vagy NameID-ben érkezett, pl. úgy, hogy az azonosítót a REMOTE_USER változóban adják ki az alkalmazás számára.

eduPersonTargetedID	
Elnevezés	**OID:** 1.3.6.1.4.1.5923.1.1.1.10
Rövid leírás	Nem átlátszó, célzott azonosító, amely nem osztható ki újra
Implementáció	kötelező
Részletes leírás	Az IdP-nek biztosítania kell, hogy egy felhasználó számára kiosztott azonosító valóban perzisztens legyen, tehát gondoskodnia kell az attribútum-értékek biztos tárolásáról - például egy megfelelő mentési tervvel üzemeltetett relációs adatbázisban. Az eduPersonTargetedID nem osztható ki újra.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Az attribútum értékének a SAML2 szabványban definiált NameID formátumúnak kell lennie; az azonosító (nem számítva az XML attribútumokat) legfeljebb 256 karakterből állhat.
Adatgazda	intézmény

Példa	Az IdP ilyen formában adja ki az azonosítót:
	
	`<saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="https://idp.example.org/idp/shibboleth" SPNameQualifier="https://sp.example.org/shibboleth"> 84e411ea-7daa-4a57-bbf6-b5cc52981b73 </saml2:NameID>`
	
	Az alkalmazás ilyen formában kapja meg az azonosítót:
	
	`https://idp.example.org/idp/shibboleth!https://sp.example.org/shibboleth!84e411ea-7daa-4a57-bbf6-b5cc52981b73`

eduPersonPrincipalName	
Elnevezés	**OID:** 1.3.6.1.4.1.5923.1.1.1.6
Rövid leírás	Állandó, nem célzott, nem újra kioszthető egyedi azonosító
Implementáció	kötelező
Részletes leírás	Formátum: <egyedi_lokális_azonosító>@<scope> Ahol ▪ **<egyedi_lokális_azonosító>**: tetszőleges állandó azonosító, amely az intézményen belül egyértelműen azonosítja a felhasználót. Kézenfekvő megoldás a felhasználói azonosító (**uid**) használata, azonban bármilyen más azonosító használható ▪ **<scope>**: egy domain, melyet az intézmény scope-ként használhat. **Megjegyzés**: az **eduPersonPrincipalName** érzékeny személyes adat, hiszen sok esetben megegyezik a felhasználó e-mail címével. Intézményen belüli használata javasolt, intézményen kívül célszerű nem átlátszó, célzott azonosítót használni.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	gipsz.jakab@example.org

Felhasználói tulajdonságokat leíró attribútumok

sn	
Elnevezés	**OID:** 2.5.4.4
Rövid leírás	A felhasználó vezetékneve
Implementáció	ajánlott
Részletes leírás	A felhasználó vezetékneve. Amennyiben több vezetékneve van a felhasználónak, akkor ezeket egyetlen értékben kell tárolni.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ Gipsz ▪ Gipszné Kiss

givenName	
Elnevezés	**OID:** 2.5.4.42
Rövid leírás	A felhasználó keresztneve
Implementáció	ajánlott
Részletes leírás	Amennyiben több keresztneve van a felhasználónak, ezeket egyetlen értékben kell tárolni.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ Jakab ▪ Mária Lujza

displayName	
Elnevezés	**OID:** 2.16.840.1.113730.3.1.241
Rövid leírás	A felhasználó megjelenítendő neve
Implementáció	ajánlott
Részletes leírás	A felhasználó neve abban a formában, ahogy a felhasználó, vagy a felhasználó intézménye meg kívánja jeleníteni.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	Gipsz Jakab Aladár

mail	
Elnevezés	**OID:** 0.9.2342.19200300.100.1.3
Rövid leírás	A felhasználó email címe
Implementáció	ajánlott
Részletes leírás	A felhasználó értesítési e-mail címe. Az így átadott email címről az intézmény biztosítja, hogy ▪ azt az intézmény biztosítja a felhasználó részére (pl neptunkod@intemzeny.hu) ▪ vagy az intézmény a cím rögzítésekor ellenőrizte, hogy az a felhasználó tulajdonában van (pl egy megerősítő levél kiküldésével). Az attribútumban ellenőrizetlen, felhasználó által megadott email címet átadni tilos.
Lehetséges értékek	Létező e-mail cím
Értékek száma	`multi`
Szintaktika	Lásd: RFC 2822
Adatgazda	nem definiált
Példa	gipsz.jakab@example.org

cn	
Elnevezés	**OID:** 2.5.4.3
Rövid leírás	A felhasználó teljes neve
Implementáció	opcionális
Részletes leírás	A felhasználó vezetéknevének és keresztnevének valamilyen módon történő, szóközzel elválasztott összefűzése. Használata intézményenként és országonként eltérő. Jellemző, hogy több értékben különböző módokon előállított értékeket is tartalmaz. **Helyette a displayName használata javasolt.**
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ Gipsz Jakab ▪ Kovács Áron;Kovacs Aron;Aron Kovacs

Felhasználó és az intézmény viszonyát leíró attribútumok

eduPersonScopedAffiliation	
Elnevezés	**OID:** 1.3.6.1.4.1.5923.1.1.1.9
Rövid leírás	Felhasználó és intézmény közti viszony leírása
Implementáció	kötelező
Részletes leírás	**<viszony>@<scope>** ▪ **<viszony>**: a felhasználó és az intézmény közti viszony leírására az alábbi értékek választhatók ▪ *student*: intézmény hallgatója ▪ *faculty*: oktatási tevékenységet végez az intézményben ▪ *staff*: nem oktatási tevékenységet végző alkalmazott (pl. a rendszergazda és a kertész is) ▪ *employee*: alkalmazott (használata intézmények között nem javasolt) ▪ *member*: azok a felhasználók, amelyek azáltal, hogy azonosította őket az IdP, rendelkeznek intézményhez kötődő általános jogosultságokkal. Jellemzően ide sorolhatók a student, faculty, staff viszonnyal rendelkezők. ▪ *affiliate*: az intézmény azonosítja őket, de nem rendelkeznek általános jogosultságokkal ▪ *alum*: öregdiák ▪ *library-walk-in*: könyvtári tag ▪ **<scope>**: egy domain, melyet az intézmény scope-ként használhat.
Lehetséges értékek	A következő értékek egyike: {student,faculty,staff,employee,member,affiliate,alum,library-walk-in}, valamint a scope
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	▪ Hallgatók: *student@example.org;member@example.org* ▪ Oktatók: *faculty@example.org;member@example.org*

eduPersonEntitlement	
Elnevezés	**OID:** 1.3.6.1.4.1.5923.1.1.1.7
Rövid leírás	A felhasználó által jogosan használt erőforrás(ok)
Implementáció	ajánlott
Részletes leírás	Azon erőforrások listája, melyet a felhasználó használhat. Sok erőforrást minden felhasználó elérhet, néhányat csak korlátozott kör - ez utóbbi esetben válik fontossá ez az attribútum
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	`urn:mace:terena.org:tcs:escience-user`

schacHomeOrganizationType	
Elnevezés	**OID:** 1.3.6.1.4.1.25178.1.2.10
Rövid leírás	Az intézmény jellege
Implementáció	opcionális
Részletes leírás	▪ **university**: Az Oktatási Minisztérium által elismert felsőoktatási intézmények (egyetemek és főiskolák) ▪ **nren**: Nemzeti kutatási és felsőoktatási kutatói hálózat szolgáltatója ▪ **library**: Könyvtárak ▪ **vho**: Virtuális azonosító szervezet egyének föderációs azonosítása céljára ▪ **school**: Általános és középiskolák ▪ **business**: Ipari vagy kereskedelmi intézmények ▪ **other**: Egyéb ▪ **test**: Teszt felhasználóról van szó
Lehetséges értékek	urn:schac:homeOrganizationType:hu:{university,nren,library,vho,school,business,other,test}
Értékek száma	`single`
Szintaktika	URN
Adatgazda	intézmény
Példa	-

Oktatásban használt attribútumok

niifPersonAttendedCourse	
Elnevezés	**OID:** 1.3.6.1.4.1.11914.0.1.164
Rövid leírás	Felhasználó által hallgatott tárgy kódja
Implementáció	opcionális
Részletes leírás	Azon tantárgyak kódja, amelyet a felhasználó az adott félévben hallgat.
Lehetséges értékek	A tanulmányi rendszerben meghatározott tantárgykódok
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	▪ VIMM1234 ▪ VIMA4321

niifEduPersonArchiveCourse	
Elnevezés	**OID:** 1.3.6.1.4.1.11914.0.1.171
Rövid leírás	A felhasználó által valaha hallgatott kurzusok
Implementáció	opcionális
Részletes leírás	Azon tantárgyak kódja, amelyet a felhasználó valaha hallgatott az adott intézményben.
Lehetséges értékek	A tanulmányi rendszerben meghatározott tantárgykódok
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	-

niifEduPersonHeldCourse	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.172
Rövid leírás	A felhasználó által aktuálisan oktatott tárgyak
Implementáció	opcionális
Részletes leírás	Azon tantárgyak kódja, amelyet a felhasználó az adott félévben (esetleg előző félévben) oktatott.
Lehetséges értékek	A tanulmányi rendszerben meghatározott tantárgykódok
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	-