Attribútum specifikáció

Verzió: 1.0.1

(2011. szeptember 14.)

aai@niif.hu

A specifikáció célja

A föderációban az IdP SAML attribútumokban ad meg adatokat a felhasználóról az SP-nek. Ahhoz, hogy az adatokban hordozott információ átadása pontos legyen, fontos, hogy a használt attribútumokat a két fél ugyanúgy értelmezze. Az attribútumok pontos meghatározása az attribútumok sémájában található. A specifikációban az alábbi sémákat használtuk fel:

- *person*, *organizationalPerson* (X.521)
- *inetOrgPerson* (RFC2798)
- *eduPerson* (http://middleware.internet2.edu/eduperson/)
- *SCHAC* (http://www.terena.org/activities/tf-emc2/schacreleases.html)
- *niifPerson*, *niifEduPerson* (NIIFSchema)

A fenti dokumentumokban definiált attribútumoknak a föderációban való *értelmezését* határozza meg az Attribútum Specifikáció. Ez néhány esetben valamivel szűkebb, mint az eredeti definíció, azért, hogy az információt az SP-k pontosabban értelmezhessék.
A specifikációban 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. Ez jelentheti azt, hogy a felhasználói adatbázisban a felhasználó bejegyzése tartalmazza ezt az attribútumot, de az attribútum más módon is előállhat (pl. statikusan vagy más attribútumokból dinamikusan generálva).
- **Attribútum kiadás**: az attribútum átadása néhány (vagy a föderációban található összes) SP-nek.
- **KÖTELEZŐ**, **AJÁNLOTT**, **OPCIONÁLIS** fogalmak meghatározását lásd a szabályozott szóhasználat leírásánál

Implementációs szintek

- **Kötelező**: az attribútumot **KÖTELEZŐ** az IdP-nek implementálni. (Nem kötelező kiadnia.)
- **Ajánlott**: az attribútumot **AJÁNLOTT** az IdP-nek implementálni, de ez néhány intézménynél lehetetlen vagy nehézségekbe ütközhet
- **Opcionális** az attribútumot az IdP a saját döntése szerint megvalósíthatja. Fontos kiemelni, hogy amennyiben egy IdP implementál egy opcionális attribútumot, azt **a specifikáció szerint KÖTELEZŐ megtennie**, azaz követve a specifikáció szemantikai és szintaktikai előírásait.

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

SP attribútum-igények

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

- **Megkövetelt**: az alkalmazás működéséhez elengedhetetlen az attribútum pl. `eduPersonPrincipalName` olyan alkalmazásokhoz, amelyek nincsenek felkészítve átlátszatlan (opaque) azonosítók kezelésére
- **Ajánlott**: az alkalmazás működését megkönnyíti az attribútum pl. a `cn` attribútum átadásakor az alkalmazás nem kéri be a felhasználó teljes nevét regisztrációkor.

Hibakezelés

Abban az esetben, ha egy IdP nem adja ki egy vagy több az SP számára elengedhetetlen attribútumot, az SP-nek KÖTELEZŐ a felhasználónak hibaüzenetet adnia. (Ugyanis egy SP csak abban az esetben jelölhet meg egy attribútumot *megkövetelt attribútumnak*, ha ez az alkalmazás működéséhez elengedhetetlen, minden egyéb esetben *ajánlott*-nak kell megjelölnie.) Azonban ez a hibaüzenet lehetséges, hogy a felhasználó számára nehezen értelmezhető (pl: *Authorization Required*).

Ezért az IdP-k számára AJÁNLOTT kiadni azokat az attribútumokat, amelyeket az SP-k *megkövetelt*-nek jelölnek meg.

Attribútumok listája

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. Erre megoldás lehet a SAML2 NameID Mapping, azonban ezt jelenleg a föderációban használt szoftverek csak részlegesen vagy egyáltalán nem támogatják.
- **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.

NameID formátumok - melyiket válasszam?

A föderáció elvárja, hogy az IdP-k támogassák mind a tranziens NameID formátumot, mind a célzott, átlátszatlan azonosítót (melyek lehetnek tároltak vagy számítottak). A tárolt azonosítót célszerű SAML2 perszistens NameID-ként kiadni, a számított azonosító azonban csak az eduPersonTargetedID attribútumban adható ki, mivel nem rendelkezik a perszisztens NameID szemantikájával.

A Shibboleth IdP implementáció esetén a számított azonosítókról a tárolt azonosítókra való áttérés nem változtatja meg a kiadott azonosítókat, ezért az SP-k számára ez az áttérés transzparens.

Ha SP-t üzemeltetünk, akkor célszerű már az üzemeltetés kezdetén eldönteni, hogy melyik formátum mellett tesszük le a voksunkat (ez elsősorban az SP által védett alkalmazás képességeitől függ), mert menet közben átállni körülményes, sok energiát igényel. A problémára reméljük könnyebb lesz a megfelelő választ megtalálni az alábbi kérdés átgondolásával:**Szükséges-e az SP számára, hogy egy-egy felhasználójához tartozzon egy-egy állandó azonosító?**

1. Ha nem, akkor egyértelmű a választás: tranziens formátumot kell használni.

2. Ha igen, és nem szükséges, hogy az állandó azonosító a felhasználóra jellemző legyen, ill. az SP mögötti alkalmazás felkészült ilyen azonosító fogadására (az alkalmazás szempontjából mindegy, hogy milyen úton, tehát eduPersonTargetedID attribútumként, vagy perzisztens NameID-ként érkezik az érték az SP-hez), akkor az SP-nek *Nem kell meghatároznia, hogy milyen NameID formátumot támogat*, hiszen ezesetben

a) Ha az IdP nem támogatja a tárolt azonosítókat, akkor a tranziens NameID mellé az eduPersonTargetedID attribútumban ki fogja adni a számított (és célzott) azonosítót.
b) Ha az IdP támogatja a tárolt azonosítókat, akkor azt perzisztens NameID-ként fogja kiadni (illetve, ha az SP kéri az eduPersonTargetedID attribútumot, az IdP képes ugyanezt a tárolt értéket ilyen formában is kiadni).

Az alkalmazáshoz mindkét esetben ugyanaz az érték jut el, mint felhasználói azonosító.

3. Ugyanaz, mint a 2., kivéve, hogy magasabb szintű felhasználókezelést (például SAML NameID menedzsmentet) is szeretne az SP használni, akkor kizárólag perzisztens NameID-t kell kérnie. A HREF föderáció jelenleg nem rendelkezik a magasabb szintű SAML protokollokról, ezért ezek használata kizárólag az adott SP és IdP közötti megállapodáson alapulhat.

4. Ha szükséges, hogy az állandó azonosító a felhasználóra jellemző legyen, őt egyértelműen azonosítsa, akkor a választás tranziens NameID, amely mellé meg kell követelni az eduPersonPrincipalName kiadását.
A HREF föderációban az IdP-k részéről elvárt, hogy a fenti 1-2. megoldásokat támogassák. A 3-4. esetében minden további nélkül előfordulhat, hogy az IdP és SP közötti kommunikáció hibát jelez, mert valamelyik fél nem támogatja a másik fél által megkövetelt / biztosított azonosító formátumot...

Megjegyzés: Egy SP a Resource Registry-ben jelezheti, hogy milyen NameID formátumokat támogat. Ha kizárólag perzisztens NameID formátumot támogat, akkor vagy kap az IdP-től ilyet, vagy hiba lép fel a válasz feldolgozása során.

eduPersonTargetedID	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonTargetedID **OID:** 1.3.6.1.4.1.5923.1.1.1.10

Rövid leírás	Nem átlátszó, újra ki nem osztható, célzott azonosító
Implementáció	kötelező
Részletes leírás	Lásd: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPTargetedID , ill. a fenti megjegyzést az implementációs szinttel kapcsolatban. Az SP a kapott értéket fel kell, hogy dolgozza, nem adhatja XML formátumban tovább az alkalmazásnak. A benne szereplő ún. qualifier-ek közül az IdP azonosítóját (`NameQualifier`) és természetesen magát az azonosítót *kötelező* szerepeltetni az alkalmazás számára átadott azonosítóban. Javasolt az egyes mezőket '!' karakterrel elválasztani egymástól. 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.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Az attribútum értékének a SAML2 szabványban definiált NameID formátumúnak kell lennie
Adatgazda	nem definiált

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	**URI:** urn:mace:dir:attribute-def:eduPersonPrincipalName **OID:** 1.3.6.1.4.1.5923.1.1.1.6
Rövid leírás	Állandó, nem célzott, nem újrakioszthatő 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>**: helyi biztonsági tartomány. A végződése kötelezően egy DNS domain, amely az IdP-t üzemeltető intézmény tulajdonában áll. **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. Az **eduPersonPrincipalName** a föderációban nem osztható ki újra.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	gipsz.jakab@example.org

niifPersonOrgID	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonPrincipalName **OID:** 1.3.6.1.4.1.11914.0.1.154
Rövid leírás	Állandó egyedi azonosító intézményen belüli, ill. e-learning használatra
Implementáció	opcionális
Részletes leírás	Bizonyos esetekben adatvédelmi szempontok miatt szükség lehet arra, hogy a felhasználó intézményen belüli azonosítója (pl. Neptun kódja) és az egyéb alkalmazásokban használt `uid` különböző legyen. Ezen attribútum intézmények közötti átadása csak abban az esetben javasolt, ha e-learning rendszerek miatt meg kell osztani a tanulmányi azonosítót.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált

Példa	-

schacPersonalUniqueCode	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.25178.1.2.14
Rövid leírás	Állandó egyedi azonosító interföderációs környezetben való használatra
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	`urn:schac:personalUniqueCode:hu:bme.hu:Neptun:gmx3f0`

Felhasználói tulajdonságokat leíró attribútumok

sn	
Elnevezés	**URI:** urn:mace:dir:attribute-def:sn **OID:** 2.5.4.4
Rövid leírás	A felhasználó vezetékneve
Implementáció	opcionális
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	**URI:** urn:mace:dir:attribute-def:givenName **OID:** 2.5.4.42
Rövid leírás	A felhasználó keresztneve
Implementáció	opcionális
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	**URI:** urn:mace:dir:attribute-def:displayname **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	**URI:** urn:mace:dir:attribute-def:mail **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

preferredLanguage	
Elnevezés	**URI:** urn:mace:dir:attribute-def:preferredLanguage **OID:** 2.16.840.1.113730.3.1.39
Rövid leírás	Előnyben részesített nyelv
Implementáció	opcionális
Részletes leírás	A felhasználó által elsődlegesen használni kívánt, általa előnyben részesített nyelv
Lehetséges értékek	RFC 2068 Language Tags szekcióban meghatározott formátumú nyelvkódok
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	hu

schacDateOfBirth	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.25178.1.2.3
Rövid leírás	A felhasználó születési dátuma
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	YYYYMMDD (RFC 3339 'full-date') formátumú dátum
Értékek száma	`single`

Szintaktika	Directory String
Adatgazda	nem definiált
Példa	19700101

schacYearOfBirth	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.1466.115.121.1.36
Rövid leírás	A felhasználó születési éve (amennyiben csak az évre van szükség, egyébként ajánlott a schacDateOfBirth használata)
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	YYYY formátumú év
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	1970

schacPersonalTitle	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.25178.1.2.8
Rövid leírás	A felhasználó személyes megszólítása.
Implementáció	opcionális
Részletes leírás	A felhasználó nevéhez kapcsolódó megszólítás, mely a teljes név elé fűzhető. A címtárban tárolható a niifPersonPrefix attribútumban is.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ Dr. ▪ Prof.

niifPersonMothersName

Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.157
Rövid leírás	Felhasználó anyja neve
Implementáció	opcionális
Részletes leírás	A felhasználó anyjának születési neve a felhasználó hivatalos irataiban.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	Kőkori Vilma

niifPersonResidentalAddress	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.159
Rövid leírás	A felhasználó állandó lakcíme
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	1111 Budapest, Villányi út 155.

homePostalAddress	
Elnevezés	**URI:** *nincs megadva* **OID:** 0.9.2342.19200300.100.1.39
Rövid leírás	A felhasználó ideiglenes lakcíme
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált

Példa	1111 Budapest, Villányi út 155.

telephoneNumber	
Elnevezés	**URI:** *nincs megadva* **OID:** 2.5.4.20
Rövid leírás	A felhasználó vezetékes telefonszáma
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	A telefonszámot az ITU-T E.123 szabványszerint kell tárolni. A melléket a / jellel elválasztva jelölhető.
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ +36 1 123 1234 ▪ +36 1 123 1234 / 102

mobile	
Elnevezés	**URI:** *nincs megadva* **OID:** 0.9.2342.19200300.100.1.41
Rövid leírás	A felhasználó mobilszáma
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	A telefonszámot az ITU-T E.123 szabványszerint kell tárolni.
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	+36 30 123 1234

eduPersonNickName	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.5923.1.1.1.2
Rövid leírás	A felhasználó beceneve
Implementáció	opcionális
Részletes leírás	Az a becenév, amelyet a felhasználó általában használ (pl.

	online fórumokon). Nem egyedi, a hossza és a tartalma sem kötött, nem állandó, ezért az alkalmazásnak mindenképpen ellenőriznie kell, mielőtt - esetleg - lokális felhasználónévként figyelembe veszi.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	felhasználó
Példa	▪ gipszj ▪ the.man.who.was.bored.to.death.by.some.american.smartguys

cn	
Elnevezés	**URI:** *nincs megadva* **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

jpegPhoto	
Elnevezés	**URI:** *nincs megadva* **OID:** 0.9.2342.19200300.100.1.60
Rövid leírás	Kis méretű fotó a felhasználóról JPEG formátumban
Implementáció	opcionális

Részletes leírás	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	-

labeledUri	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.250.1.57
Rövid leírás	Felhasználóhoz tartozó URI-k
Implementáció	opcionális
Részletes leírás	A felhasználó által megadott, vagy rá valamilyen formában jellemző URI-k (gyakran URL-ek) gyűjteménye, mint pl. a személyes honlapjának címe. Minden azonosítóhoz opcionálisan kapcsolható szöveges leírás.
Lehetséges értékek	Az URL-t urlencode-olva kell tárolni (RFC 2079).
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	▪ http://example.com/%7Euser/foo Foo page ▪ ftp://ftp.example.com

Felhasználó és az intézmény viszonyát leíró attribútumok

eduPersonScopedAffiliation	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonScopedAffiliation **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 **Megj:** lehetséges, hogy a föderációban használható értékek körét a későbbiekben szűkíteni fogjuk ▪ **<scope>**: egy domain, melyet az intézmény scope-ként használhat. Lásd még: http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html#eduPersonAffiliation
Lehetséges értékek	A következő értékek egyike: {student,faculty,staff,employee,member,affiliate,alum,library-walk-in}, valamint a scope **Megj**: lehetséges, hogy a föderációban használható értékek körét a későbbiekben szűkíteni fogjuk **<scope>**: helyi biztonsági tartomány. A végződése kötelezően egy DNS domain, amely az IdP-t üzemeltető intézmény tulajdonában áll. Lásd még: http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html#eduPersonAffiliation
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	▪ Hallgatók: *student@example.org;member@example.org* ▪ Oktatók: *faculty@example.org;employee@example.org;member@example.org* ▪ Nem alkalmazott oktató-hallgatók: *student@example.org;faculty@example.org;member@example.org*

eduPersonEntitlement	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonEntitlement **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:geant:niif.hu:niif:entitlement:vhoadmin

schacHomeOrganizationType	
Elnevezés	**URI:** urn:mace:dir:attribute-def:schacHomeOrganizationType **OID:** 1.3.6.1.4.1.25178.1.2.10
Rövid leírás	Az intézmény jellege
Implementáció	kötelező
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	-

ou	
Elnevezés	**URI:** urn:mace:dir:attribute-def:ou **OID:** 2.5.4.11
Rövid leírás	Az intézményen belüli egység teljes neve (organizationalUnit)
Implementáció	opcionális
Részletes leírás	Azon egység (tanszék, intézet, könyvtár, stb) neve, amelyhez a felhasználó tartozik.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	Directory String
Adatgazda	nem definiált
Példa	Automatizálási és alkalmazott informatikai tanszék

eduPersonOrgUnitDN	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonOrgUnitDN **OID:** 1.3.6.1.4.1.5923.1.1.1.4
Rövid leírás	A felhasználóhoz tartozó szervezeti egység azonosítója
Implementáció	ajánlott
Részletes leírás	A felhasználóhoz tartozó szervezeti egység (pl. tanszék, intézet, könyvtár, ...) intézményen belüli egyedi, esetleg hierarchikusan képzett azonosítója. Amennyiben az adott felhasználó több egységhez is besorolható, ez az attribútum több értéket is tartalmazhat.
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	DN
Adatgazda	intézmény
Példa	▪ ou=VIK,ou=Units,o=BME,c=hu

	▪ ou=AAIT,ou=VIK,ou=Units,o=BME,c=hu ▪ ou=MIT,ou=VIK,ou=Units,o=BME,c=hu

eduPersonOrgUnitDN	
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonPrimaryOrgUnitDN **OID:** 1.3.6.1.4.1.5923.1.1.1.8
Rövid leírás	A felhasználóhoz hozzárendelhető elsődleges szervezeti egység azonosítója.
Implementáció	opcionális
Részletes leírás	Az #eduPersonOrgUnitDN-ben tárolt egység-azonosítók közül azon elem, amelyhez a felhasználó elsődlegesen köthető.
Lehetséges értékek	Egy olyan azonosító, mely szerepel az #eduPersonOrgUnitDN értékei között.
Értékek száma	`single`
Szintaktika	DN
Adatgazda	intézmény
Példa	ou=AAIT,ou=VIK,ou=Units,o=BME,c=hu

Oktatásban használt attribútumok

niifPersonAttendedCourse	
Elnevezés	**URI:** urn:geant:niif.hu:dir:attribute-def:niifEduPersonAttendedCourse **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. Oktatási intézmény esetén JAVASOLT az attribútumot implementálni és az intézményen belüli SP-k számára kiadni. Adatvédelmi szempontból JAVASOLT az értékeket úgy szűrni, hogy az SP csak a számára releváns tárgyak kódját kapja meg.
Lehetséges értékek	A tanulmányi rendszerben meghatározott tantárgykódok
Értékek száma	`multi`
Szintaktika	Directory String

Adatgazda	intézmény
Példa	▪ VIMM1234 ▪ VIMA4321

niifEduPersonArchiveCourse	
Elnevezés	**URI:** *nincs megadva* **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	-

niifEduPersonMajor	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.162

Rövid leírás	A hallgató főszakja
Implementáció	opcionális
Részletes leírás	A hallgató főszakja - a http://www.mab.hu/listak2.html címen található lista alapján
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	▪ műszaki informatikus mérnök ▪ elméleti fizikus

niifEduPersonFaculty	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.160
Rövid leírás	Kar neve
Implementáció	opcionális
Részletes leírás	Teljes neve annak a karnak, amelyhez a hallgató tartozik
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	Villamosmérnöki és Informatikai Kar

niifEduPersonFacultyDN	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.161
Rövid leírás	A hallgató karának DN-je
Implementáció	opcionális
Részletes leírás	Annak a karnak a DN-je, amelyhez a hallgató tartozik. Ajánlott a kezdőpont alatt található `ou=Units` alá tenni az egyes karokat (lásd #eduPersonOrgUnitDN)
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`

Szintaktika	DN
Adatgazda	intézmény
Példa	ou=VIK,ou=Units,o=BME,c=hu

niifEduPersonStudentCategory	
Elnevezés	**URI:** *nincs megadva* **OID:** 1.3.6.1.4.1.11914.0.1.174
Rövid leírás	Tanuló/hallgató képzési szintjének meghatározása
Implementáció	opcionális
Részletes leírás	A hallgató képzési szintjének pontosabb meghatározása (az eduPersonScopedAffiliation kiegészítése) ▪ **bachelor**: bachelor képzésben részt vevő hallgató (javasolt affiliation: student,member) ▪ **master**: master képzésben részt vevő hallgató (javasolt affiliation: student,member) ▪ **doctor**: doktori képzésben részt vevő hallgató (javasolt affiliation: student,member) ▪ **exchange-student**: vendéghallgató (javasolt affiliation: student,member) ▪ **qualifying-studies**: előkészítős hallgató (javasolt affiliation: member) ▪ **open-university**: nyílt egyetemi képzésben részt vevő hallgató (javasolt affiliation: affiliate) Ha egy hallgató nem sorolható be egyik kategóriába sem (pl. nem bolognai rendszer szerint tanul), akkor az attribútum ne kapjon értéket!
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	Directory String
Adatgazda	intézmény
Példa	-