HREF/eduID föderációhoz kapcsolódó tudnivalók

- HREF
- HREFContract
- HREF műszaki előírások
- HREFChecklist
- HREF alapelvek és alapvető szabályok
- HREF attribútum specifikáció
- HREFJoin
- HREF szolgáltatási szint megállapodás
- HREFServices
- HREF Key Rollover 2020
- HREF Key Rollover 2020 English
- HREF Key Rollover 2025
- HREF Key Rollover 2025 English
- Federation Policy
- HREFUseCaseStub
- Sirtfi
- HREFPolicyStub
- HREFMetadataRegistrationPracticeStatement
- HREF metadata specifikáció
- FederationStats
- HREFGlossary
- URN

- URN SCHAC
- URN Registry

HREF

Magyarországi felsőoktatási és kutatói föderáció (Hungarian Research & Education Federation)

A föderáció jelenleg *technikai pilot* státuszban van, azaz elsősorban a technikai együttműködésre, ill. a hosszú távú szabályozás előkészítésére koncentrálunk.

Tagjai

- Debreceni Egyetem
- Dunaújvárosi Főiskola
- ELTE
- Georgikon Keszthely
- MTA KFKI Csillebérc
- MTA Sztaki
- NIIF Intézet
- PPKE
- ZMNE

Szolgáltatások

URN

Támogatott szabványok

A föderáció a SAML2 szabvány protokolljait használja. Minden résztvevő támogatja a SAML2 SSO Profile-t HTTP POST bindingon keresztül, néhányan Artifact bindingon keresztül is. A legtöbb résztvevő támogatja a SAML2 Single Logout profile-t.

HREFContract

A HREF Föderáció nem jogi személy, így a szerződést formálisan a Föderációs Operátor és a Tag illetve a Partner kötik. A csatlakozáshoz szükséges egy egyoldalú szándéknyilatkozat aláírása is.

A dokumentumok letölthetők eduid.hu/dokumentumok oldalról.

A szerződés az alábbi dokumentumokra hivatkozik:

- Szószedet: a szerződésben és a vonatkozó dokumentumokban használt fogalmak meghatározása. Glossary
- Alapelvek: a HREF Föderáció működésének alapvető szabályai Federation Policy
- Műszaki előírások:
  - IdP műszaki követelmények; IdP Operation Requirements
  - SP műszaki követelmények; SP Operation Requirements
- Szolgáltatási szint megállapodás: a Föderációs Operátor szolgáltatásai és ezek vállalt paraméterei. Service Level Agreement
- Attribútum specifikáció: a felhasználói attribútumok cseréjét meghatározó leírás. Attribute Specification
- Metadata specifikáció: a metaadatok használatának és értelmezésének szabályai. Metadata Specification
- Föderációs szolgáltatások: a föderáció Tagjai és Partnerei által a Föderációban üzemeltetett szolgáltatások. Definition of Federated Services

HREF m?szaki el?írások

A dokumentum célja, hogy a HREF Föderációhoz csatlakozó Tagok és Partnerek számára elvárásokat és ajánlásokat fogalmazzon meg, melyek a csatlakozáshoz szükséges identitás-menedzsment, valamint üzemeltetési területeket fednek le.

A dokumentumban a **KÖTELEZŐ**, **TILOS**, **AJÁNLOTT**, **NEM AJÁNLOTT** kifejezések értelmezése az alábbiak szerinti:

- **KÖTELEZŐ** (ill. **"KÖTELES"**, **"kell"**) jelentése: a pontban leírtak betartása a föderációba vetett bizalom kiépítéséhez és megtartásához elengedhetetlenül szükségesek, ettől a résztvevők nem térhetnek el;
- **TILOS** jelentése KÖTELEZŐ NEM, azaz a pontban leírtak szerint az intézmény nem járhat el;
- az **AJÁNLOTT** pontoktól való eltéréseket az intézmények dokumentálni kötelesek.
- **NEM AJÁNLOTT** jelentése: amennyiben az intézmény a pontban leírtak szerint jár el, ezt dokumentálni köteles.

1. Identitás-menedzsment

- 1.1. Az intézmény köteles adatkezelési elveit dokumentálni, azt a felhasználókkal megismertetni.
- 1.2. Az intézmény köteles a felhasználóiról általa ismert adatok forrását, karbantartásának módját, illetve ezen adatok becsült adatminőségét dokumentálni, és igény esetén ezt a dokumentációt a föderáció tagjainak rendelkezésére bocsátani.
- 1.3. Kötelező a felhasználónevek egyediségét biztosítani.
- 1.4. Egy természetes személyhez nem ajánlott több felhasználói azonosítót rendelni.
- 1.5. Nem ajánlott szerep felhasználók (dékán, igazgató) használata.
- 1.6. Attribútumok használata:
  - 1.6.1. A megvalósított attribútumokat az IdP-nek az Attribútum Specifikációban leírt módon kell megvalósítani;
  - 1.6.2. Az IdP-nek kötelező megvalósítania az alábbi attribútumokat:
    - eduPersonTargetedID
    - eduPersonPrincipalName
    - eduPersonScopedAffialiation
  - 1.6.3. Az IdP-nek ajánlott megvalósítania az alábbi attribútumokat:
    - displayName
    - mail
    - sn
    - givenName

    - 1.6.4. Az IdP-nek kötelező biztosítania, hogy az eduPersonTargetedID és az eduPersonPrincipalName attribútumok ne legyenek újra kioszthatók.
- 1.7. Teszt felhasználók az alábbi megkötések mentén használhatóak:
    - 1.7.1. minden teszt felhasználót egyértelműen azonosítani és dokumentálni kötelező (az érte felelős munkatárssal együtt),
    - 1.7.2. teszt felhasználóval valós tranzakciót kezdeményezni tilos, kivéve, ha a tranzakcióban részt vevő SP a teszt felhasználó használatához hozzájárult,
    - 1.7.3. ajánlott ezen felhasználókat a megfelelő homeOrganizationType értékkel megkülönböztetni.
- 1.8. Felhasználói azonosító adatokat (pl. jelszó) publikus hálózaton titkosítatlanul továbbítani (felhasználótól bekérni, adatbázisszerver felé kommunikálni) tilos.
- 1.9. A felhasználói jelszavakat ajánlott nem elektronikus formában kiosztani (pl. személyesen, vagy postai úton).
- 1.10. A felhasználók intézményhez fűződő viszonyában bekövetkezett változásokat 7 napon belül kötelező megjeleníteni az IdP adatbázisában és az eduPersonScopedAffiliation attribútum értékében.
    - 1.10.1. Amennyiben az intézmény külső adatforrást (tanulmányi- ill. bérügyi rendszert) használ a felhasználói adatok tárolására, úgy ez a 7 napos korlát a hiteles adat elsődleges rendszerben történő megváltozásától számítandó.

2. Szolgáltatás-menedzsment

- 2.1. Az intézmény köteles a föderációs operátorral való kapcsolattartásra megfelelő szerepkört kialakítani. Ajánlott a kapcsolattartáshoz szerep e-mail címet megadni.
- 2.2. IdP-t üzemeltető intézmény köteles az IdP-vel kapcsolatban végfelhasználói támogatást nyújtani, és ezen támogatás elérhetőségéről a felhasználóit tájékoztatni.
- 2.3. Az intézmény köteles az általa üzemeltett IdP forgalmi adataiból anonimizált, legalább napi felbontású adatokat szolgáltatni a föderációs operátor számára föderációs célú statisztika készítésének céljából.

3. Üzemeltetési kérdések

- 3.1. A személyes adatokkal kapcsolatos tranzakciókról kötelező naplóállományt készíteni, és azt legalább 30 napig megőrizni.
- 3.1.1. Az intézmény ezeket a naplókat köteles a hatályos adatvédelmi szabályokkal összhangban kezelni.
- 3.2. Az AAI infrastruktúra komponensei esetén kötelező legalább 2048 bites kulcsok használata.
    - 3.2.1. Biztosítani kell a privát kulcsok védelmét.
    - 3.2.2. Amennyiben egy kulcs kompromittálódik, az intézmény köteles a föderációs operátort 24 órán belül értesíteni.
    - 3.2.3. Ajánlott hosszú lejáratú, self-signed tanúsítványok használata.
- 3.3. Vonatkozó SAML szabványok

    - 3.3.1. Kötelező az *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* (http://saml2int.org) dokumentumban kötelezőnek megjelölt elemek támogatása
    - 3.3.2. Ajánlott a SAML2 Single Logout profil támogatása HTTP-Redirect illetve SOAP binding felett.
- 3.4. Az IdP köteles minden végpontját HTTPS (SSL/TLS) protokollok segítségével védeni.
- 3.5. Az IdP minden SAML végpontjának az IdP-t üzemeltető intézmény tulajdonában álló DNS domainnek, vagy az alatt levő névnek kell lennie.
- 3.6. Az IdP által használt scope-oknak az IdP-t üzemeltető intézmény tulajdonában álló DNS domainnek, vagy az alatt levő névnek kell lennie.

HREFChecklist

El?zetes ellen?rzés

Az alábbi listán haladunk végig egy-egy csatlakozási kérelem beérkeztekor, és ennek eredményének figyelembe vételével hozza meg a Tagok Tanácsa a döntést a felvételről.

- Adatkezelés
  - Van-e adatkezelési szabályzat?
  - A felhasználókról szóló, intézmény által ismert adatok forrása, karbantartásának módja dokumentált-e? (**TAG**)
  - Elérhetők-e a fenti dokumentumok? A hivatkozásnak a metadata állományban kell szerepelnie.
  - Ezek megfelelnek-e a Föderációs alapelvek-ben foglaltaknak?
- Műszaki követelmények
  - Az intézmény teljesíti-e a Műszaki előírásokat leírtakat? (Műszaki előírások IdP-k számára, Műszaki előírások SP-k számára)
  - Van-e kijelölt ember, aki a föderációs ügyekért felelős, technikailag be tud avatkozni (be tud-e lépni a Resource Registry-be és a saját IdP-jét adminisztrálni is tudja)?
  - Van-e jól beállított naplózási mechanizmus?
  - Megfelelőek-e az entitás által használt kulcsok?
  - Megfelelőek-e az entitás által támogatott SAML-profilok?
  - Az attribútumspecifikációnak megfelelő-e az attribútumok használata?
  - Ajánlásoktól eltéréseket dokumentálni
- Egyéb
  - Hány felhasználót tud az IdP azonosítani?
  - Elvárt, hogy az entitás technikai kapcsolattartója iratkozzon fel a href-tech levelezőlistára, az entitás adminisztratív kapcsolattartója pedig a href-admin levelezőlistára.

HREF alapelvek és alapvet? szabályok

Föderációs alapelvek

1. A föderáció célja, hogy a felhasználók úgy vehessenek igénybe szolgáltatásokat - amennyiben erre jogosultak -, hogy a saját intézményük azonosítja őket.
2. Az IdP csak abban az esetben azonosít egy felhasználót, ha az illető valamilyen - ismert - viszonyban van az intézménnyel.
3. Az IdP és az SP nem ad meg magáról hamis, félrevezető információt.
4. Az IdP minden tőle telhetőt megtesz annak érdekében, hogy a kiadott információ a lehető legpontosabb legyen. Az SP tisztában van vele, hogy bizonyos információkat a felhasználók maguk is szerkeszthetnek.
5. Az IdP gondoskodik róla, hogy a felhasználót azonosító információk (pl. jelszó) védett módon legyenek tárolva, ill. a felhasználók ezt biztonságosan adhassák meg.
6. Az SP csak a működéséhez minimálisan szükséges adatmennyiséget (attribútumokat) igényli a felhasználóról.
7. Az SP nem kérheti a felhasználót, hogy adja meg az IdP-nél érvényes jelszavát.
8. Az SP-nél történő adatkezelés a törvényi előírások szerint működik.
9. Felhasználói visszaélések vizsgálatában az IdP és az SP együttműködik egymással.
10. Az IdP és az SP az informatikai rendszereit az elvárható gondossággal üzemelteti.

Szabályok

Adatvédelmi szabályok

1. A Tag és a Partner biztosítja, hogy a HREF Föderáció működése során közöttük a személyes adatok kezelése a vonatkozó jogszabályoknak megfelelő módon történik. Így a személyes adatok kezelése csak törvényi felhatalmazáson vagy felhasználói önkéntes, határozott és tájékozott hozzájárulásán alapul, amellyel beleegyezését fejezi ki az őt érintő személyes adatok kezelésébe.
2. Mind a Tag, mind a Partner rendelkezik a személyes adatok kezelését megfelelően rendező adatkezelési szabályzattal, amely rendelkezik különösen:
   - a kezelt személyes adatok köréről;
   - az adatkezelés céljáról;
   - az adatkezelés időtartamáról;

- az adatalanyokat érintő tiltakozási jog lehetőségéről.

3. Mind a Tag, mind a Partner a mindenkor hatályos adatkezelési szabályzatukat elérhetővé teszik.

Üzemeltetési szabályok

1. Az üzemeltetéssel kapcsolatos szabályokat, valamint a megkövetelt és ajánlott eljárásokat külön dokumentumok részletezik: en_US IdP üzemeltetési szabályok, SP üzemeltetési szabályok
2. A Föderációs Operátor jogosult ellenőrizni a vonatkozó szabályok betartását.
3. A Tag és a Partner gondoskodik arról, hogy a metaadatok kezelése a metadata specifikációnak megfelelően történjen, így:
   - a Tag a Resource Registry használatával gondoskodik arról, hogy az őt érintő föderációs metaadatok naprakészek legyenek,
   - a metaadatokat a specifikációnak megfelelő gyakorisággal frissítik és ellenőrzik.
4. A felhasználói attribútumok átadása során az IdP és a SP az attribútum specifikáció előírásait betartják.

Adatkezeléssel kapcsolatos szabályok

1. Az Azonosító Szervezet biztosítja, hogy a felhasználó regisztrációs folyamatai dokumentáltak legyenek.
2. Csak olyan felhasználó azonosítható, akinek az intézményhez való viszonya egyértelműen megállapítható.
3. Adatminőség
   - A személyes adat tárolási módjának alkalmasnak kell lennie arra, hogy az érintett felhasználót csak a tárolás céljához szükséges ideig lehessen azonosítani.
   - Az adatminőség biztosítása érdekében az IdP AAI Kapu számára hozzáférhetővé tett felhasználói adatokat célszerű autoritatív adatbázisban rögzített adatok alapján létrehozni, így a rendszeres frissítéssel azok időszerűsége, pontossága nem vitatott.
   - Amennyiben az IdP AAI Kapu adatbázisa nem autoritatív adatbázis alapján működik, a Tagnak meg kell tennie a szükséges lépéseket az adatminőség biztosítása érdekében.
4. Az Azonosító Szervezet törekszik arra, hogy a HREF Föderáció szolgáltatásai minden jogosult felhasználója számára elérhetővé váljon.
5. Az Azonosító Szervezet biztosítja, hogy az IdP AAI Kapu az attribútum specifikációban megkövetelt attribútumokat megvalósítsa.

Tagsággal kapcsolatos szabályok

A HREF Föderáció infrastruktúrájának üzemeltetője az országos kutatói hálózatot működtető Föderációs Operátor. A HREF Föderáció további résztvevői egy már megkötött csatlakozási szerződés alapján a Tagok és a Partnerek.

1. A föderáció **Tagjai** az alábbi intézmények lehetnek:
   - felsőoktatási intézmények;
   - akadémiai intézmények, kutatással foglalkozó intézmények;
   - oktatással foglalkozó intézmények;
   - közgyűjtemények.
2. A föderáció **Partnere** tetszőleges szervezet lehet
3. A föderáció Tagjai és Partnerei jogosultak a föderációban szolgáltatásokat üzemeltetni
4. A Partner a Tagok Tanácsa ülésein megfigyelőként részt vehet, azonban szavazati joggal nem rendelkezik.
5. Csak Tagok jogosultak:
   - felhasználói adatokat szolgáltatni;
   - a Tagok Tanácsába szavazati joggal rendelkező képviselőt küldeni.

HREF attribútum specifikáció

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). Az implementáció részleteivel kapcsolatban a föderáció nem fogalmaz meg megkötést
- **Attribútum kiadás**: az attribútum átadása néhány (vagy a föderációban található összes) SP-nek.

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.

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

Lista

Kötelez? attribútumok

eduPersonScopedAffiliation

schacHomeOrganizationType
eduPersonPrincipalName

Ajánlott attribútumok

mail
eduPersonEntitlement

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...

> **Info**
>
> 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

	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**, **célzott** azonosító, amely **nem osztható ki újra**
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. Az eduPersonTargetedID **nem osztható ki újra**.

	eduPersonTargetedID
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.

Példa	Az IdP ilyen formában adja ki az azonosítót:
	`<saml2:NameID xmlns:saml2="urn:oasis:names:tc:`
	`Format="urn:oasis:names:tc:SAML:2.0:nameid-`
	`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

	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 újra kioszthatő** egyedi azonosító
Implementáció	kötelező

	eduPersonPrincipalName
Részletes leírás	Formátum: <egyedi_lokális_azonosító>@ 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 • : 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**. Bizonyos alkalmazások nem támogatják a különleges karaktereket az azonosítókban, ezért a föderációban az eduPersonPrincipalName kizárólag alfanumerikus karaktereket, pont ('.'), kötőjel ('-') és alulvonás ('_') karaktereket tartalmazhat.
Lehetséges értékek	nincs korlátozás
Értékek száma	`single`
Szintaktika	`Directory String`
Adatgazda	intézmény
Példa	gipsz.jakab@example.org

niifPersonOrgID

	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

	niifPersonOrgID
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`

schacPersonalUniqueCode

	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`
Példa	`urn:schac:personalUniqueCode:hu:bme.hu:Neptun:gmx3f0`

Felhasználói tulajdonságokat leíró attribútumok

sn

	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

	sn
Értékek száma	`single`
Szintaktika	`Directory String`
Példa	• Gipsz • Gipszné Kiss

givenName

	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`
Példa	• Jakab • Mária Lujza

displayName

	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`
Példa	Gipsz Jakab Aladár

mail

	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](http://www.faqs.org/rfcs/rfc2822.html)`
Példa	gipsz.jakab@example.org

preferredLanguage

	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`
Példa	hu

schacDateOfBirth

	schacDateOfBirth
Elnevezés	**URI:** nincs megadva **OID:** 1.3.6.1.4.1.25178.1.2.3

	schacDateOfBirth
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`
Példa	19700101

schacYearOfBirth

	schacYearOfBirth
Elnevezés	**URI:** nincs megadva **OID:** 1.3.6.1.4.1.25178.1.0.2.3
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`
Példa	1970

schacPersonalTitle

	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`

	schacPersonalTitle
Példa	• Dr. • Prof.

niifPersonMothersName

	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`
Példa	Kőkori Vilma

niifPersonResidentalAddress

	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`
Példa	1111 Budapest, Villányi út 155.

homePostalAddress

	homePostalAddress
Elnevezés	**URI:** nincs megadva **OID:** 0.9.2342.19200300.100.1.39
Rövid leírás	A felhasználó ideiglenes lakcíme

	homePostalAddress
Implementáció	opcionális
Részletes leírás	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	`Directory String`
Példa	1111 Budapest, Villányi út 155.

telephoneNumber

	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 szabvány szerint kell tárolni. A melléket a `/` jellel elválasztva jelölhető.
Értékek száma	`multi`
Szintaktika	`Directory String`
Példa	• +36 1 123 1234 • +36 1 123 1234 / 102

mobile

	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 szabvány szerint kell tárolni.
Értékek száma	`multi`
Szintaktika	`Directory String`
Példa	+36 30 123 1234

eduPersonNickName

	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

	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`
Példa	• Gipsz Jakab • Kovács Áron;Kovacs Aron;Aron Kovacs

jpegPhoto

	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`

labeledUri

	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`
Példa	• http://example.com/%7Euser/foo Foo page • ftp://ftp.example.com

Felhasználó és az intézmény viszonyát leíró attribútumok

eduPersonScopedAffiliation

	eduPersonScopedAffiliation
Elnevezés	**URI:** urn:mace:dir:attribute-def:eduPersonScopedAffiliation **OID:** 1.3.6.1.4.1.5923.1.1.1.9

	eduPersonScopedAffiliation
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 **Megjegyzés:** 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://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonAffiliation Egy lehetséges vizuális ábrázolás, azonban a halmazok pontos meghatározása az intézmény feladata.
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

	eduPersonScopedAffiliation
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

	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 > **Info** Az eduPersonEntitlement attribútumnak csak azon értékeit szabad kiadni az SP-nek, amelyek rá vonatkoznak. Ennek meghatározása kézi adminisztráció esetén igen nehéz lehet, ezért erre célszerű valamilyen adminisztrációs felületet használni. (Sajnos jelenleg nem létezik ilyen alkalmazás.)
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	`Directory String`
Adatgazda	intézmény
Példa	urn:geant:niif.hu:niif:entitlement:vhoadmin

schacHomeOrganizationType

	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

ou

	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`
Példa	Automatizálási és alkalmazott informatikai tanszék

eduPersonOrgUnitDN

	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	opcionális
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

eduPersonPrimaryOrgUnitDN

	eduPersonPrimaryOrgUnitDN
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

Oktatásban használt attribútumok

niifEduPersonAttendedCourse

	niifPersonAttendedCourse
Elnevezés	**URI:** urn:geant:niif.hu:dir:attribute-def:niifEduPersonAttendedCourse **OID:** 1.3.6.1.4.1.11914.0.1.164

	niifPersonAttendedCourse
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

	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

niifEduPersonHeldCourse

	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

	niifEduPersonHeldCourse
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

niifEduPersonMajor

	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 mab.hu oldalán található lista alapján
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	`Directory String`
Adatgazda	intézmény
Példa	• műszaki informatikus mérnök • elméleti fizikus

niifEduPersonFaculty

	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

	niifEduPersonFaculty
Példa	Villamosmérnöki és Informatikai Kar

niifEduPersonFacultyDN

	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	-
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	`DN`
Adatgazda	intézmény

niifEduPersonStudentCategory

	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!

	niifEduPersonStudentCategory
Lehetséges értékek	nincs korlátozás
Értékek száma	`multi`
Szintaktika	`Directory String`
Adatgazda	intézmény

HREFJoin

Az eduID föderációhoz való csatlakozás folyamata

1. A csatlakozni kívánó tag/partner jelzi csatlakozási szándékát a Föderációs Operátor felé.
2. Mind jogilag, mind technikailag előkészül a csatlakozáshoz: Föderáció alapelvek, Műszaki előírások IdP-k számára, Műszaki előírások SP-k számára.
3. Egyeztetés után elküldi az aláírt szerződést, ill. nyilatkozatot, és ezzel párhuzamosan elérhetővé teszi a csatlakozás előtti ellenőrzéskor átnézendő dokumentumokat. Különösen fontos, hogy megadja az azonosítható felhasználók számát és elérhetővé tegye az adatkezelési szabályzatát.
4. A Föderációs Operátor elkészíti a Tag számára a szükséges HEXAA jogosultságokat
5. A Föderációs Operátor elvégzi az előzetes ellenőrzést (a különálló és benyújtandó dokumentumokat és a Resource Registry-be felvitt adatokat), majd ennek eredményértől tájékoztatja a Tagok Tanácsát
6. Tagok Tanácsa dönt a csatlakozni kívánó tag/partner kérelméről
7. A Föderációs Operátor - pozitív TT döntés esetén - aláírva visszaküldi a szerződést, és beteszi a föderációs éles metaadatba az új entitást. Negatív válasz esetén a hiányosságok ismertetése mellett lehetőséget biztosít azok a pótlására, javítására.

Azonosító szervezet (IdP) felvétele a föderációba

1. A Föderációs Operátor az intézményi adminisztrátorral egyeztetve rögzíti a Resource Registry-be az IdP adatait. Egyúttal a Föderációs Operátor az IdP-t hozzáadja a föderációs tesztmetaadathoz, ezáltal az intézményi adminisztrátor, amennyiben helyesen konfigurálta az IdP-t, be fog tudni lépni a Resource Registrybe.
2. A Tagok Tanácsa dönt az IdP felvételi kérelméről. Pozitív döntés esetén a Föderációs Operátor hozzáadja az éles föderációs metaadathoz az IdP-t.

Intézményi (tagi) szolgáltatás (SP) felvétele a föderációba

1. Egy intézményi adminisztrátor (akinek a HEXAA-ban megfelelő, a Resource Registryhez szükséges intézményi admin joggköre van) a Resource Registry-ben rögzíti az SP minden szükséges adatát.
2. Az SP a föderációs metaadatba a Föderációs Operátor számára történt jelézés után kerülhet. Technikailag a Föderációs Operátor engedélyezi a föderációs metaadatba történő megjelenést.

Külső (partner) szolgáltatás (SP) felvétele a föderációba

1. A Föderációs Operátor a Resource Registry-ben rögzíti az SP minden szükséges adatát.
2. A Tagok Tanácsa pozitív döntése után a Föderációs Operátor engedélyezi az új SP föderációs metaadatba történő megjelenését.
3. Az SP-n a későbbiekben szükségessé váló módosításokat a Föderációs Operátor végzi el.

HREF szolgáltatási szint megállapodás

M?szaki szolgáltatások

Metadata

A metadata a föderáció tagjait leíró, a föderációs operátor által digitálisan aláírt állomány, mely létfontosságú a résztvevők egymással való kommunikációjának szempontjából. A metadata által tartalmazott információkkal és a metadata biztonságával kapcsolatban további információkat a Metadata Specifikáció tartalmaz.

Elérhet?ség kritériumai

A legfontosabb szempont, hogy az elérhetetlenségből fakadó szolgáltatáskiesés megakadályozható legyen. A föderációban részt vevő komponensek a központi metadatát helyileg gyorstárazzák, így a metadata elérhetetlensége a gyorstárazási idő (`cacheDuration`) alatt nem okozhat szolgáltatáskiesési problémát - kivéve azon entitások esetén, melyek a kiesés időtartama alatt kerülnek újraindításra.

Fontos kiemelni, hogy a központi metadata elérhetetlensége miatti szolgáltatáskiesés bármely föderációs komponensnél a fent leírt gyorstárazási és érvényességi időszakon belül mindenképpen helyi szoftver- (vagy konfigurációs) hiba következménye.

A metadata akkor tekinthető **elérhetőnek**, ha legalább egy, a föderációs operátor hálózatán kívül levő IP címről elérhető, és az URL-ről egy szabványos SAML metadata állomány tölthető le, és aláírása egy ismert kulccsal ellenőrizhető. A metadata akkor tekinthető **aktuálisnak**, ha elérhető, és a letöltött állomány 2 óránál nem régebben keletkezett.

Vállalt rendelkezésre állás

A föderációs operátor vállalja, hogy a metadata tetszőleges 12 hónapos időtartamra nézve az idő **99.9%-ában elérhető**, **99%-ában aktuális**.

Föderáció adminisztráció (Resource Registry)

A Resource Registry a metaadat állományban található - az egész föderációt leíró - adatok szerkesztését lehetővé tevő alkalmazás. A Resource Registryben tárolt adatokat a föderációs

operátor illetve az intézmények kapcsolattartói szerkeszthetik.

Elérhet?ség kritériumai

A Resource Registry elérhetősége a benne tárolt adatok szerkesztésére vonatkozik, a metaadatok elérhetőségét nem érinti. Mivel azonban az esetleges kompromittálódott kulcsok visszavonása az intézmények részéről csak ezen az adminisztrációs rendszeren keresztül elvégezhető, ezért a rendszer elérhetősége a föderáció operatív működése szempontjából fontos.

A Resource Registry elérhető, ha legalább egy, a föderációs operátor hálózatán kívül eső IP címről megnyitható, és bejelentkezés működőképes (feltételezve, hogy az azonosító szervezet rendben működik).

Vállalt rendelkezésre állás

Tetszőleges 12 hónapos időtartamra nézve a szolgáltatás az idő **98%-ában** elérhető.

Discovery Service

A Discovery Service (keresőszolgáltatás) az SP-k számára a felhasználó azonosító szervezetét kiválasztó alkalmazás. Amennyiben egy SP adminisztrátora úgy dönt, hogy az SP a központi keresőszolgáltatást használja, úgy az adott SP-n történő belépések esetén a komponens elérhetősége kritikus.

A keresőszolgáltatás a metaadatokból dolgozik, a metaadat változásait 1 napon (24 órán) belül átveszi.

Elérhet?ség kritériumai

A keresőszolgáltatás elérhetőnek tekintendő, ha legalább 1, föderációs operátor hálózatán kívül eső IP címről elérhető, és a protokoll által leírt működést mutatja, valamint a metadatában szereplő azonosító szervezeteket ajánlja fel (figyelembe véve az előző pontban leírt időkorlátot a módosítások átvezetésére).

Vállalt rendelkezésre állás

Tetszőleges 12 hónapos időtartamra nézve a szolgáltatás az idő **99.9%-ában** elérhető.

Virtuális azonosítószervezet

A föderációs operátor által biztosított virtuális azonosítószervezet biztosítja a saját azonosítószervezettel nem rendelkező intézmények számára a felhasználók AAI infrastruktúrába kapcsolását, illetve a többi azonosítószervezet számára a vendégfelhasználók regisztrálását és karbantartását.

Elérhet?ség kritériumai

A virtuális azonosítószervezet két komponensből áll:

- adminisztrációs felület a felhasználók kezelésére
- azonosító szerver

A virtuális azonosítószerv elérhetőnek tekinthető, ha legalább egy, föderációs operátor hálózatán kívül eső IP címről elérhető az adminisztrációs felület (feltéve, hogy az adminisztrátor saját azonosító szervezete és a föderációs infrastruktúra megfelelően működik); illetve az azonosító szerver.

Vállalt rendelkezésre állás

A virtuális azonosítószervezet elérhető tetszőleges, 12 hónapos időtartamon számított teljes idő **99%-ában**.

Föderációs komponensek monitorozása

A föderációs operátor az általa üzemeltetett komponenseket folyamatosan és automatikusan ellenőrzi. Ez az ellenőrzés kiterjed az infrastruktúra építőelemeire (switchek, hálózati elemek, szerverek), a szervereken futó operációs rendszerekre, és a föderációs szoftverekre is.

A monitorozás az NIIF hálózatán (HBONE) belülről történik.

Támogatás

Helpdesk intézményi adminisztrátorok számára

A föderációs operátor ügyfélszolgáltatot tart fenn a tagok és partnerek számára. Az ügyfélszolgálat feladata mind az incidensek kezelése, mind az általános segítségnyújtás (például csatlakozási szándék, vagy hibaelhárítás esetén).

Az ügyfélszolgálat **munkanaponként 09-17 óra között** működik, és az intézményi megkeresésekre legfeljebb 1 munkanapon belül válaszol.

Az esetleges incidensek 0-24 óráig bejelenthetők az NIIFI incidens-kezelő ügyeletén is (http://www.niif.hu/szolgaltatasok/middleware/csirt_kapcsolat).

Egyéb támogatás

A föderációs operátor a föderációs technológiákkal, trendekkel kapcsolatban folyamatosan frissülő tudásbázist tart fent, illetve rendszeres és eseti oktatásokkal segíti a tagok közötti tudásátadást. Ugyancsak elősegíti a használt szoftverekkel kapcsolatos információk, hibabejelentések terjedését

a résztvevő intézmények és a szoftverek fejlesztői között. Az operátor feladata, hogy a felhasznált szoftverekkel kapcsolatos biztonsági frissítésekre felhívja a résztvevők figyelmét.

Kiegészít? szolgáltatások

A föderációs operátor az alábbi szolgáltatásokat garancia nélkül, best effort jelleggel működteti:

- URN registry (URN névterek kezelése, delegálása)
- Statisztika
- Audit
- Intézményi AAI komponensek monitorozása
- IdP és SP hosting

HREFServices

Föderációs Szolgáltatások

Tagi Szolgáltatások

A Tag az alábbi szolgáltatásokat regisztrálhatja a Föderációba:

- **Azonosító Szolgáltatás (Identity Provider, IdP)**: a tag felhasználóinak azonosítását végző szolgáltatás. Az Azonosító Szolgáltatás szabványos protokollon elérhető a Tartalomszolgáltatások számára.
- **Tartalomszolgáltatás (Service Provider, SP)**: a Föderáció Tagjainak felhasználói számára nyújtott szolgáltatások vagy elérhetővé tett erőforrások.
- **Attribútum Szolgáltatás (Attribute Authority, AA)**: bizonyos felhasználói adatok Tartalomszolgáltatók általi lekérdezését speciális esetekben (pl. virtuális szervezet, VO) lehetővé tevő szolgáltatás.

Partner Szolgáltatások

A Partner az alábbi szolgáltatásokat regisztrálhatja a Föderációba:

- **Tartalomszolgáltatás (Service Provider, SP)**: a Föderáció Tagjainak felhasználói számára nyújtott szolgáltatások vagy elérhetővé tett erőforrások.

HREF Key Rollover 2020

Bevezetés

A HREF új metaadat aláírókulcsra áll át a SAML 2.0 metaadataiban (HREF-2020). A HREF szövetségi tagoknak és partnernek az új aláírókulcshoz tartozó konfigurációkat 2022. január 1.-ig frissíteniük kell az összes eduID.hu-t támogató rendszerükben. Ezt követően a régi - több, mint 6 éves aláírókulcs (HREF-2011) - leállításra kerül, és az utolsó aláírástól számított 10. napon a régi metaadat érvénytelen lesz.

Az alábbi táblázatok az átálláshoz szükséges összes adatot tartalmazzák. A konfigurációs példák, olyan megoldásokat kínálnak (ahol ez lehetséges), amelyekkel egyszerre lehet használni a régi és az új metaadatot.

Key Rollover

Elnevezések

Elnevezés	Metaadat aláíró tanúsítvány	Kivezetés tervezett időpontja
HREF-2011	href-metadata-signer-2011.crt	2022.01.01.
HREF-2015	mdx-test-signer-2015.crt	2022.01.01.
HREF-2020	href-metadata-signer-2020.crt	2025.06.14.

SHA1 fingerprints

Elnevezés	SHA1 fingerprint
HREF-2011	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
HREF-2015	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
HREF-2020	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`

Domain név változások

Domain	Technikai domain	Kulcs	Állapot
metadata.eduid.hu	`metadata.eduid.hu/2011/href.xml`	HREF-2011	Prod
metadata.eduid.hu	`metadata.eduid.hu/2020/href.xml`	HREF-2020	Prod
mdx.eduid.hu	`mdx-2015.eduid.hu`	HREF-2015	Prod
mdx.eduid.hu	`mdx-2020.eduid.hu`	HREF-2020	Prod

Shibboleth Service Provider beállítások

https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider

XML

https://wiki.shibboleth.net/confluence/display/SP3/XMLMetadataProvider

```
<MetadataProvider type="Chaining">
    <MetadataProvider type="XML" id="href-2011" url="https://metadata.eduid.hu/2011/href.xml"
backingFilePath="href-2011.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
    <MetadataProvider type="XML" id="href-2020" url="https://metadata.eduid.hu/2020/href.xml"
backingFilePath="href-2020.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
</MetadataProvider>
```

MDX

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/SP3/MDQMetadataProvider

```
<MetadataProvider type="MDQ" id="href-2015" ignoreTransport="true" baseUrl="https://mdx-
2015.eduid.hu/">
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
```

```
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<MetadataProvider type="MDQ" id="href-2020" ignoreTransport="true" baseUrl="https://mdx-2020.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
```

Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2015" ignoreTransport="true">
    <Subst>https://mdx-2015.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
    <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
```

Shibboleth Identity Provider beállítások

XML

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>
```

```
</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

MDX

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2020.eduid.hu/</MetadataQueryProtocol>
```

```
</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2020.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

SimpleSAMLphp

MDX

```
//config/config.php
'metadata.sources' => [[=> 'flatfile']('type'), // ez a *-hosted metadata konfiguráció
betöltése miatt szükséges
    [
        'type' => 'mdq',
        'server' => 'https://mdx-2020.eduid.hu',
        /* --- */
        'validateFingerprint' => 'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61'
    ],
],
```

metarefresh

https://simplesamlphp.org/docs/stable/simplesamlphp-maintenance#section_3

https://github.com/simplesamlphp/simplesamlphp-module-metarefresh/blob/master/docs/simplesamlphp-automated_metadata.md

```
// config/config-metarefresh.php
$config = [
  'sets' => [
      'href-2011' => [
          'cron'      => ['hourly'],
          'sources'   => [
              [
                  'src' => 'https://metadata.eduid.hu/2011/href.xml',
                  'validateFingerprint' =>
'FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66',
              ],
          ],
          'expireAfter'       => 777600, // 9 nap
          'outputDir'     => 'metadata/metarefresh-href-2011/',
          'outputFormat' => 'flatfile',
      ],
      'href-2020' => [
          'cron'      => ['hourly'],
          'sources'   => [
              [
                  'src' => 'https://metadata.eduid.hu/2020/href.xml',
                  'validateFingerprint' =>
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61',
              ],
          ],
          'expireAfter'       => 777600, // 9 nap.
          'outputDir'     => 'metadata/metarefresh-href-2020/',
          'outputFormat' => 'flatfile',
      ],
   ],
];
```

```
// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2011'],
```

```
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
],
```

FAQ /GYIK

Bővítés alatt!

- Miért cserél KIFÜ kulcsot?
- IdP-t érinti?
- Mi a helyzet az eduGAIN-t használó IdP-kkel?
- Mi a helyzet az eduGAIN-t használó SP-kkel?
- Hogyan tudom ellenőrízni, hogy jó kulcsot használok?

HREF Key Rollover 2020 English

Introduction

The Hungarian Research and Educational Federation is migrating to a new metadata signing certificate (HREF-2020).

All HREF member and partner have to update their IdP and SP configurations before 2022. January 1st., in order to provide the federational services without interruption. After 2022 January 1st., the old metadata signing certificate (HREF-2011) will be shut down.

The tables below and configuration examples are containing all the necessary technical information.

Key Rollover

Code names

Code name	Metadata signing certificate	Date of expiration
HREF-2011	href-metadata-signer-2011.crt	2022.01.01.
HREF-2015	mdx-test-signer-2015.crt	2022.01.01.
HREF-2020	href-metadata-signer-2020.crt	2025.06.14.

SHA1 fingerprints

Code name	SHA1 fingerprint
HREF-2011	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
HREF-2015	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
HREF-2020	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`

Domain names

Domain	URL	Key	Status
metadata.eduid.hu	`metadata.eduid.hu/2011/href.xml`	HREF-2011	Prod
metadata.eduid.hu	`metadata.eduid.hu/2020/href.xml`	HREF-2020	Prod
mdx.eduid.hu	`mdx-2015.eduid.hu`	HREF-2015	Prod
mdx.eduid.hu	`mdx-2020.eduid.hu`	HREF-2020	Prod

Shibboleth Service Provider Configurations

https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider

XML

https://wiki.shibboleth.net/confluence/display/SP3/XMLMetadataProvider

```
<MetadataProvider type="Chaining">
    <MetadataProvider type="XML" id="href-2011" url="https://metadata.eduid.hu/2011/href.xml"
backingFilePath="href-2011.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
    <MetadataProvider type="XML" id="href-2020" url="https://metadata.eduid.hu/2020/href.xml"
backingFilePath="href-2020.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
</MetadataProvider>
```

MDX

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/SP3/MDQMetadataProvider

```
<MetadataProvider type="MDQ" id="href-2015" ignoreTransport="true" baseUrl="https://mdx-2015.eduid.hu/">
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<MetadataProvider type="MDQ" id="href-2020" ignoreTransport="true" baseUrl="https://mdx-2020.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
```

Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2015" ignoreTransport="true">
    <Subst>https://mdx-2015.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
    <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
```

Shibboleth Identity Provider Configurations

XML

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>
```

```
    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

MDX

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
```

```
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2020.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2020.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2020.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

SimpleSAMLphp Configurations

MDX

```
//config/config.php
'metadata.sources' => [[=> 'flatfile']('type'), // ez a *-hosted metadata konfiguráció
betöltése miatt szükséges
     [
         'type' => 'mdq',
         'server' => 'https://mdx-2020.eduid.hu',
         /* --- */
         'validateFingerprint' =>
```

```
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61'
     ],
],
```

metarefresh

https://simplesamlphp.org/docs/stable/simplesamlphp-maintenance#section_3

https://github.com/simplesamlphp/simplesamlphp-module-metarefresh/blob/master/docs/simplesamlphp-automated_metadata.md

```
// config/config-metarefresh.php
$config = [
   'sets' => [
       'href-2011' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2011/href.xml',
                   'validateFingerprint' =>
'FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap
           'outputDir'     => 'metadata/metarefresh-href-2011/',
           'outputFormat' => 'flatfile',
       ],
       'href-2020' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2020/href.xml',
                   'validateFingerprint' =>
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap.
           'outputDir'     => 'metadata/metarefresh-href-2020/',
           'outputFormat' => 'flatfile',
```

```
        ],
    ],
];
```

```
// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2011'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
],
```

HREF Key Rollover 2025

Bevezetés

A HREF új metaadat aláírókulcsra áll át a SAML 2.0 metaadataiban (HREF-2025). A HREF szövetségi tagoknak és partnernek az új aláírókulcshoz tartozó konfigurációkat 2025. juniús 14.-ig frissíteniük kell az összes eduID.hu-t támogató rendszerükben. Ezt követően a régi - több, mint 4 éves aláírókulcs (HREF-2020) - leállításra kerül, és az utolsó aláírástól számított 10. napon a régi metaadat érvénytelen lesz.

Az alábbi táblázatok az átálláshoz szükséges összes adatot tartalmazzák. A konfigurációs példák, olyan megoldásokat kínálnak (ahol ez lehetséges), amelyekkel egyszerre lehet használni a régi és az új metaadatot.

Key Rollover

Elnevezések

Elnevezés	Metaadat aláíró tanúsítvány	Kivezetés tervezett időpontja
HREF-2011	[https://metadata.eduid.hu/certs/href-metadata-signer-2011.crt href-metadata-signer-2011.crt]	2022.01.01.
HREF-2015	[https://metadata.eduid.hu/certs/mdx-test-signer-2020.crt mdx-test-signer-2015.crt]	2022.01.01.
HREF-2020	[https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt href-metadata-signer-2020.crt]	2025.06.14.
HREF-2025	[https://metadata.eduid.hu/certs/href-metadata-signer-2025.crt href-metadata-signer-2025.crt]	2030.06.14.

SHA1 fingerprints

Elnevezés	SHA1 fingerprint
HREF-2011	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`

Elnevezés	SHA1 fingerprint
HREF-2015	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
HREF-2020	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`
HREF-2025	`45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE`

Domain név változások

Domain	Technikai domain	Kulcs	Állapot
metadata.eduid.hu	`metadata.eduid.hu/2011/href.xml`	HREF-2011	Prod
	`metadata.eduid.hu/2020/href.xml`	HREF-2020	Prod
	`metadata.eduid.hu/2025/href.xml`	HREF-2025	Prod
mdx.eduid.hu	`mdx-2015.eduid.hu`	HREF-2015	Prod
	`mdx-2020.eduid.hu`	HREF-2020	Prod
	`mdx-2025.eduid.hu`	HREF-2025	Prod

Discovery Service változások

URL
https://mdx-2020.eduid.hu/role/idp.ds
https://mdx-2025.eduid.hu/discovery/ds

Shibboleth Service Provider beállítások

https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider

XML

https://wiki.shibboleth.net/confluence/display/SP3/XMLMetadataProvider

```
<MetadataProvider type="Chaining">
    <MetadataProvider type="XML" id="href-2020" url="https://mdx-2020.eduid.hu"
```

```
backingFilePath="href-2020.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
    <MetadataProvider type="XML" id="href-2025" url="https://mdx-2025.eduid.hu"
backingFilePath="href-2025.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
</MetadataProvider>
```

MDX

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/SP3/MDQMetadataProvider

```
<MetadataProvider type="MDQ" id="href-2020" ignoreTransport="true" baseUrl="https://mdx-
2020.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<MetadataProvider type="MDQ" id="href-2025" ignoreTransport="true" baseUrl="https://mdx-
2025.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
```

példa

apache + shibboleth 3.X - sed segítségével

```
sudo sed 's/mdx-2020.eduid.hu/mdx-2025.eduid.hu/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-2020/href-2025/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-metadata-signer-2020.crt/href-metadata-signer-2025.crt/g'
/etc/shibboleth/shibboleth2.xml -i
sudo sed 's#https://mdx-202..eduid.hu/role/idp.ds#https://mdx-2025.eduid.hu/discovery/ds#g'
/etc/shibboleth/shibboleth2.xml -i
sudo systemctl restart shibd.service apache2.service
```

Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
    <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2025" ignoreTransport="true">
    <Subst>https://mdx-2025.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
</MetadataProvider>
```

Shibboleth Identity Provider beállítások

XML

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2025.xml"
                  metadataURL="https://metadata.eduid.hu/2025/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2025.xml"
```

```
                    metadataURL="https://metadata.eduid.hu/2025/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

MDX

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                    connectionRequestTimeout="PT2S"
                    connectionTimeout="PT2S"
                    socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                    connectionRequestTimeout="PT2S"
```

```
                    connectionTimeout="PT2S"
                    socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

SimpleSAMLphp

MDX

```
//config/config.php
'metadata.sources' => [
     ['type' => 'flatfile'], // ez a *-hosted metadata konfiguráció betöltése miatt szükséges
     [
         'type' => 'mdq',
         'server' => 'https://mdx-2025.eduid.hu',
         /* --- */
         'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE'
     ],
],
```

metarefresh

https://simplesamlphp.org/docs/stable/simplesamlphp-maintenance#section_3

https://github.com/simplesamlphp/simplesamlphp-module-metarefresh/blob/master/docs/simplesamlphp-automated_metadata.md

```
// config/config-metarefresh.php
$config = [
```

```
   'sets' => [
       'href-2020' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2020/href.xml',
                   'validateFingerprint' =>
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap.
           'outputDir'     => 'metadata/metarefresh-href-2020/',
           'outputFormat' => 'flatfile',
       ],
       'href-2025' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2025/href.xml',
                   'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap.
           'outputDir'     => 'metadata/metarefresh-href-2025/',
           'outputFormat' => 'flatfile',
       ],
    ],
];
```

```
// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2025'],
],
```

FAQ /GYIK

Bővítés alatt!

- Miért cserél KIFÜ kulcsot?
- IdP-t érinti?
- Mi a helyzet az eduGAIN-t használó IdP-kkel?
- Mi a helyzet az eduGAIN-t használó SP-kkel?
- Hogyan tudom ellenőrízni, hogy jó kulcsot használok?

HREF Key Rollover 2025 English

Introduction

The Hungarian Research and Educational Federation is migrating to a new metadata signing certificate (HREF-2025).

All HREF members and partners must update their IdP and SP configurations with the new signing certificate by June 14, 2025, in order to ensure uninterrupted access to federated services supporting eduID.hu. After this date, the old signing certificate (HREF-2020), which has been in use for more than 4 years, will be decommissioned, and 10 days after its last use, the old metadata will become invalid.

The tables below contain all necessary data for the transition. Where possible, configuration examples offer solutions that allow simultaneous use of both the old and new metadata.

Key Rollover

Code names

Code name	Metadata signing certificate	Date of expiration
HREF-2011	[https://metadata.eduid.hu/certs/href-metadata-signer-2011.crt href-metadata-signer-2011.crt]	2022.01.01.
HREF-2015	[https://metadata.eduid.hu/certs/mdx-test-signer-2020.crt mdx-test-signer-2015.crt]	2022.01.01.
HREF-2020	[https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt href-metadata-signer-2020.crt]	2025.06.14.
HREF-2025	[https://metadata.eduid.hu/certs/href-metadata-signer-2025.crt href-metadata-signer-2025.crt]	2030.06.14.

SHA1 fingerprints

Code name	SHA1 fingerprint
HREF-2011	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
HREF-2015	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
HREF-2020	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`
HREF-2025	`45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE`

Domain names

Domain	URL	Key	Status
metadata.eduid.hu	`metadata.eduid.hu/2011/href.xml`	HREF-2011	Prod
	`metadata.eduid.hu/2020/href.xml`	HREF-2020	Prod
	`metadata.eduid.hu/2025/href.xml`	HREF-2025	Prod
mdx.eduid.hu	`mdx-2015.eduid.hu`	HREF-2015	Prod
	`mdx-2020.eduid.hu`	HREF-2020	Prod
	`mdx-2025.eduid.hu`	HREF-2025	Prod

Discovery Service change

URL
https://mdx-2020.eduid.hu/role/idp.ds
https://mdx-2025.eduid.hu/discovery/ds

Shibboleth Service Provider beállítások

https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider

XML

https://wiki.shibboleth.net/confluence/display/SP3/XMLMetadataProvider

```
<MetadataProvider type="Chaining">
    <MetadataProvider type="XML" id="href-2020" url="https://mdx-2020.eduid.hu"
backingFilePath="href-2020.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
    <MetadataProvider type="XML" id="href-2025" url="https://mdx-2025.eduid.hu"
backingFilePath="href-2025.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
</MetadataProvider>
```

MDX

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/SP3/MDQMetadataProvider

```
<MetadataProvider type="MDQ" id="href-2020" ignoreTransport="true" baseUrl="https://mdx-
2020.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<MetadataProvider type="MDQ" id="href-2025" ignoreTransport="true" baseUrl="https://mdx-
2025.eduid.hu/">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
```

példa

apache + shibboleth 3.X - sed segítségével

```
sudo sed 's/mdx-2020.eduid.hu/mdx-2025.eduid.hu/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-2020/href-2025/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-metadata-signer-2020.crt/href-metadata-signer-2025.crt/g'
/etc/shibboleth/shibboleth2.xml -i
sudo sed 's#https://mdx-202..eduid.hu/role/idp.ds#https://mdx-2025.eduid.hu/discovery/ds#g'
/etc/shibboleth/shibboleth2.xml -i
```

```
sudo systemctl restart shibd.service apache2.service
```

Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
    <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2025" ignoreTransport="true">
    <Subst>https://mdx-2025.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
</MetadataProvider>
```

Shibboleth Identity Provider beállítások

XML

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2025.xml"
                  metadataURL="https://metadata.eduid.hu/2025/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/FileBackedHTTPMetadataProvider

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/href-2025.xml"
                  metadataURL="https://metadata.eduid.hu/2025/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

MDX

Shibboleth 4.X

https://wiki.shibboleth.net/confluence/display/IDP4/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

Shibboleth 3.X

https://wiki.shibboleth.net/confluence/display/IDP30/DynamicHTTPMetadataProvider

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
                  connectionRequestTimeout="PT2S"
                  connectionTimeout="PT2S"
                  socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

SimpleSAMLphp

MDX

```
//config/config.php
'metadata.sources' => [
     ['type' => 'flatfile'], // ez a *-hosted metadata konfiguráció betöltése miatt szükséges
     [
         'type' => 'mdq',
         'server' => 'https://mdx-2025.eduid.hu',
         /* --- */
         'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE'
     ],
],
```

metarefresh

https://simplesamlphp.org/docs/stable/simplesamlphp-maintenance#section_3

https://github.com/simplesamlphp/simplesamlphp-module-metarefresh/blob/master/docs/simplesamlphp-automated_metadata.md

```
// config/config-metarefresh.php
$config = [
   'sets' => [
       'href-2020' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2020/href.xml',
                   'validateFingerprint' =>
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap.
           'outputDir'     => 'metadata/metarefresh-href-2020/',
           'outputFormat' => 'flatfile',
       ],
       'href-2025' => [
           'cron'      => ['hourly'],
           'sources'   => [
               [
                   'src' => 'https://metadata.eduid.hu/2025/href.xml',
                   'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE',
               ],
           ],
           'expireAfter'       => 777600, // 9 nap.
           'outputDir'     => 'metadata/metarefresh-href-2025/',
           'outputFormat' => 'flatfile',
       ],
    ],
];
```

```
// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2025'],
],
```

FAQ /GYIK

Bővítés alatt!

- Miért cserél KIFÜ kulcsot?
- IdP-t érinti?
- Mi a helyzet az eduGAIN-t használó IdP-kkel?
- Mi a helyzet az eduGAIN-t használó SP-kkel?
- Hogyan tudom ellenőrízni, hogy jó kulcsot használok?

Federation Policy

About eduID

Hungarian Research and Educational Federation (HREF) is a SAML2-based Identity Federation of Hungarian higher education and research institutions, public collections and other content providers. For the end-users, the federation aims to be transparent, therefore the login procedure is communicated as ***eduID login***.

Contacts

The Federation is operated by Pro-M (successor of KIFÜ which is successor of NIIF Institute) as a Federation Operator. Questions, concerns or any kind of requests about the Federation should be directed to any of the following addresses:

- **eduid@pro-m.hu**
- **Péter Molnár and János Mohácsi**, *Pro-M* 35 Váci út H-1134 Budapest Hungary

News and information about the federation is published at http://eduid.hu (Hungarian only)

Policy and principles of interoperation

Basic principles

1. The aim of the Federation is to allow the use of services of its Members and Partners, where authorisation is based on the user information originating from the users' Home Institutions.
2. Home Institutions must only authenticate users having a known affiliation to them.
3. IdPs and SPs must not give false or misleading information about themselves.
4. User information provided by IdPs should be as accurate as possible. SPs must take into account that parts of the received information may be at the discretion of the user.
5. User credentials (i.e. passwords) stored by IdPs must be protected and verified only through secure procedures.
6. SPs must request only the user attributes which are absolutely necessary for their operation.
7. SPs must not ask users for their federation passwords.

8. SPs must handle personal data according to the local privacy laws.
9. IdPs and SPs must cooperate in the investigation of possible abuse/fraud.
10. IT systems running IdPs and SPs must be operated with due diligence.

Data protection

- Prior joining the federation, every entity needs to publish the Data Protection Policy under which it operates. This policy must be kept up-to-date.
- Whenever the Data Protection Policy changes, the Federation Operator must be notified.
- Transfer of personal data is only allowed when either
  - authorised by law, or
  - the user expressed his or her consent on the data transfer.

Rules of membership

The Federation is operated by the Federation Operator, that also operates the national research network. Further participants are *Members* and *Partners* that must have a signed contract with the Operator.

1. The following institutions may be **Members** of the federation:
   - Institutions of the higher education;
   - Institutions of the Hungarian Research Academy and other research institutions;
   - Institutions of secondary education;
   - Public collections.
2. Any organisation might join as a **Partner**.
3. All Members and Partners of the Federation might provide services.
4. A Partner might participate in the meeting of the Members' Board as an observer, without having rights to vote.
5. Only Members are entitled to
   - supply user identity information to the federation
   - send representatives into the Members' Board with a right to vote.

Governance

The governance body of the federation is the **Members' Board (MB)**. Every Federation Member may send one representative person to the Members' Board, who has one vote.

The working language of the MB is Hungarian. The Board publishes its decisions and guidelines at http://eduid.hu/dokumentumok in Hungarian, although whenever the topic is of interest of any international Partner, it shall be translated to English and the administrative contacts shall be notified.

MB is authorised to

- accept new Federation documents or modify existing ones,
- accept application of new Members and Partners

Partners may also send representatives for MB meetings, without voting rights.

Legal

The Federation itself is not a legal entity, Members and Partners establish a legal connection to the Federation Operator. Any legal claims between Members and/or Partners shall be directed to the organisation operating the Identity Provider or the Service Provider.

HREFUseCaseStub

NIIF AAI felhasználási lehet?ségek

Szolgáltatások	Hallgatóknak	Oktatóknak	Adminisztratív személyzet részére
Internetelérés nem csak az anyaintézményben	+	+	+
Online könyvtári szolgáltatások	+	+	+
Online elérhető szakmai folyóiratok	+	+	+
Tudás adatbázisok (tananyagok)	+	+	
Statisztikai adatbázisok	+	+	
Speciális keresési szolgáltatások	+	+	+
Hírszolgáltatások	+	+	+
Elektronikus oktatási (e-learning) szolgáltatások	+	+	+
Tanulmányi rendszerek	+	+	
Elektronikus vizsgáztatási rendszerek	+	+	
Számlázási, könyvelési szolgáltatások			+
Erasmusos diákok VHO-s azonosítása	+		
Külföldi oktatóknak biztosított szolgáltatások VHO-s azonosítása		+	+
Közösségépítő szolgáltatások (Sample Use Case)	+	+	
Hallgatói önkormányzatok saját szolgáltatásai	+		
Utazás iroda által nyújtott szolgáltatások	+	+	+

Szolgáltatások	Hallgatóknak	Oktatóknak	Adminisztratív személyzet részére
Online rendelhető termékekre diák vagy oktatói kedvezmények (pl. jegyrendelés (mozijegy, koncert stb.)	+	+	
Kollégiumokkal kapcsolatos szolgáltatások (adatbázis, jelentkezés stb.)	+		+
HR szolgáltatások		+	+
Projektszemléletű jogosultságok kezelése	+	+	+
Telekommunikációs és informatikai szolgáltatások (pl. tárhely, domain név)	+	+	
Marketing szolgáltatások, online felmérések	+	+	+
Egyéb			

Sirtfi

Security Incident Response Trust Framework for Federated Identity (SIRTFI)

A SIRTFI kezdeményezést a REFEDS (the Research and Education FEDerations group) koordinálja, célja, hogy a föderációs és különösen a föderációközi együttműködéshez kapcsolódó incidenskezelés számára kereteket szabjon, a föderációban résztvevő felek számára egy magasabb biztonsági szintet adjon azáltal, hogy a SIRTFI-nak megfelelő entitások kapcsán biztosak lehetnek az alábbiakban:

- az intézményi üzemeltető az adott entitáshoz kapcsolódó biztonsági frissítéseket, mind operációs rendszer, mind kapcsolódó szoftverek, mind pedig a föderációs együttműködést megvalósító middleware tekintetében a lehető leggyorsabban telepíti,
- biztosított intézményi szinten az incidenskezeléshez kapcsolódó kompetencia, mellyel párhuzamosan az intézmény föderációs szinten (a metadatán keresztül) megjelöl egy speciális elérhetőséget, melyen keresztül az esetleges biztonsági incidensek kapcsán biztosan felvehető a kapcsolat a kompetens intézményi személlyel,
- az adott entitáshoz kapcsolódóan megfelelő naplózás történik, szükség esetén visszakereshetők az esetleges incidensekhez kapcsolódó alapvető információk,
- az adott intézmény rendelkezik AUP-val és biztosítja, hogy felhasználói be is tartják.

Fontos, hogy a SIRTFI-képesség metadatában való jelzése önbevallás útján történik, tehát föderációs szinten nem kerül vizsgálatra, hogy az intézmény az állításának megfelelően ténylegesen bír-e a fenti listában jelzett kompetenciákkal. Az eduID entitások kapcsán a Resource Registry-ben állítható be a SIRTFI-képesség.

HREFPolicyStub

Általános elvárások

- A Tag és Partner az NIIFI-vel az NIIF AAI üzemeltetése érdekében folyamatosan együttműködik, különösen az NIIF AAI-val összefüggésben felmerülő visszaélések kivizsgálása érdekében.
- Az NIIF AAI Operátor a föderáció zavartalan üzemeltetése érdekében utólagos monitoring vizsgálatot végezhet, amely során jogosult ellenőrizni:
  - az Üzemeltetéssel kapcsolatos műszaki elvárások és feltételekben meghatározott kötelezettségek betartását;
  - azonosítási eljárások megfelelőségét;
  - a hatályban lévő adatvédelmi és felhasználói szabályzatnak a Tagok Tanácsa Ajánlásainak megfelelő módosítását;
  - a Tagok Tanácsa egyéb Ajánlásainak való megfelelést.
- A Tag biztosítja, hogy a Metadata mindenkor csak az aktuális adatokat tartalmazza, ennek érdekében évente önellenőrzést végez.

Adatvédelmi elvárások

- A Tag és a Partner biztosítja, hogy az NIIF AAI működése során közöttük a személyes adatok kezelése a vonatkozó jogszabályoknak megfelelő módon történik. Így különösen:
  - a személyes adatok kezelése csak törvényi felhatalmazás vagy felhasználói önkéntes, határozott és tájékozott hozzájárulásán alapul, amellyel beleegyezését fejezi ki az őt érintő személyes adatok kezelésébe.
  - a Tag vagy a Partner által üzemeltetett föderációs szolgáltatás csak a működtetéséhez feltétlenül szükséges adatokat igényli a felhasználókról
- Mind az Tag, mind a Partner rendelkezik a személyes adatok kezelését megfelelően rendező adatkezelési szabályzattal, amely rendelkezik különösen:
  - a kezelt személyes adatok köréről;
  - az adatkezelés céljáról;
  - az adatkezelés időtartamáról;
  - az adatalanyokat érintő tiltakozási jog lehetőségéről.
- Mind a Tag, mind a Partner a mindenkor hatályos adatkezelési szabályzatukat, egy az NIIF AAI által fenntartott központi helyen elérhetővé teszik.
- A Tag biztosítja, hogy csak olyan saját szolgáltatást (Saját SP) regisztrál a Metadatába, amely
  - tiszteletben tartja az NIIF AAI működtetését megalapozó alapelveket továbbá;

    - betartja az Üzemeltetéssel kapcsolatos műszaki elvárások és feltételekben foglalt kötelezettségek, az ott meghatározott feltételeknek már az NIIF AAI-hez való csatlakozás pillanatában, továbbá az NIIF AAI tagsága során mindvégig megfelel;
    - az üzemeltetéssel kapcsolatos műszaki elvárások és feltételekben foglalt kötelezettségeknek való folyamatos megfelelés érdekében feliratkozik az NIIF AAI Operátor által üzemeltetett levelezőlistára, valamint folyamatosan kapcsolatot tart az NIIF AAI Operátorral és az NIIF AAI többi résztvevőjével;
    - biztosítja az azonosítási eljárások megfelelőségét és elérhetőségét;
    - az Üzemeltetéssel kapcsolatos műszaki elvárások és feltételekben foglalt kötelezettségek elmulasztásából eredő károkért teljes körű felelősséggel tartozik;
    - betartja az NIIF AAI működését szabályozó kötelező dokumentumok (Csatlakozási Szerződés, Szabályzat) vonatkozó rendelkezéseit.
- A Tag felelősséget vállal, hogy a Saját SP vállalt kötelezettségeinek eleget tesz, továbbá ezen kötelezettségeinek elmulasztásából eredő károkért teljes körű felelősséggel tartozik.
- Adatminőség
    - z adatkezelés során a személyes adat felvételének és kezelésének nemcsak tisztességesnek és törvényesnek kell lennie, de az így rögzített adatnak pontosnak, teljesnek, és ha szükséges időszerűnek is kell lennie.
    - személyes adat tárolási módjának alkalmasnak kell lennie arra, hogy az érintett felhasználót csak a tárolás céljához szükséges ideig lehessen azonosítani.
    - z adatminőség biztosítása érdekében az Idp AAI adatbázis adatait authoritatív adatbázisban rögzített adatok alapján célszerű létrehozni, így az adatok folyamatosan frissülésével azok időszerűsége, pontossága nem vitatott.
    - mennyiben nem az IdP AAI adatbázis nem autoratív adatbázis alapján működik az Tagnak meg kell tennie a szükséges lépéseket az adatminőség biztosítása érdekében.

Identitás kezeléssel kapcsolatos elvárások

- A Tag biztosítja, hogy a Felhasználó regisztrációs folyamata, továbbá az NIIF AAI regisztrációjának törlése megfelelően dokumentált legyen.
- Az Tag mindent megtesz annak érdekében, hogy az általa kiadott személyes adatok megfeleljenek az adatminőség törvényi követelményeinek, így azok pontosak és időszerűek legyenek.
    - A Tag IdP AAI kapuja által szolgáltatott identitás-csoportokat (pl. hallgatók, oktatók) teljes módon kell nyilvántartani, így ennek megfelelően pl. nem csak egy csoportjuk számára szolgáltat TO DO
    - A Tag a felhasználói identitáskezelés körében biztosítja, hogy a Felhasználók adataiban, ill. státuszában bekövetkezett változtatásoknak a változástól illetve a változás bejelentésétől számított 7 napon belül megjeleníti az NIIF AAI attribútumokban.

    - Státusz adatok esetében a változást követő 7. napon;
    - Személyi adatok esetében a változás bejelentéstől számított 7. napon;
    - Szervezeti kapcsolódás adatait illetően a kapcsolódást elsődlegesen nyilvántartó rendszerben bekövetkező változástól számított 14. nap;
    - Oktatással kapcsolatos adatok esetben az oktatási adatokat elsődlegesen nyilvántartó rendszerben bekövetkező változástól számított 30. napon.
- A Tag biztosítja, hogy az IdP AAI Kapu az attribútum specifikációban megkövetelt attribútumokat megvalósítsa.

A Tag és Partner egyéb kötelezettségei az NIIF AAI üzemeltetés érdekében

- A Tag az NIIF AAI megfelelő üzemeltetés érdekében biztosítja, hogy az IdP AAI Kapu a Felhasználó azonosítását követően kiadja az attribútumokat (ARP) az SP AAI Kapu részére.
- A Partner feltünteti a Resource Registry-ben a megkövetelt, ill. opcionális attribútumok körét, továbbá az NIIF AAI-ban történő részvétele során biztosítja, hogy az így megadott adatok mindig naprakészek legyenek.

HREFMetadataRegistrationPracticeStatement

Metadata Registration Practice Statement

Federation Name: eduID Federation Operator: NIIFI, Hungary Federation Web Page:

http://www.eduid.hu

Date of last change: 20110907

Common Practices

All IdP, SP and RRA [1] administrators connect via https and authenticate via eduID to the Resource Registry, where the original information gets administrated which is later used for generating the federation metadata.

In addition, before the federation operator publishes metadata dedicated for interfederation, an institution has first to declare that its processes are ready for interfederation. Only then the federation operator will be able to declare that their respective entity is also technically ready to participate in interfederation.

Practices on Identity Provider Registration

An IdP registering to the federation needs to be manually approved by the Members' Board. Such approval requires:

- a completed membership service agreement signed by official representative(s) of the newly participating institution
- elements and attributes to be registered must use a domain name of that institution

Subsequent changes to these elements and attributes do not require re-approval by the federation operator. Only, administrators appointed specifically by that institution can modify the IdP specific information.

Practices on Service Provider Registration

Each SP must be manually approved by an RRA Administrator in order to be registered with the federation. RRA Administrators must be from the institution on whose behalf the SP gets registered.

It is the duty of the RRA Administrator to review and approve all the details provided by the SP administrator. In addition, an RRA Administrator can reject changes or further modify details of an SP before approving it.

After approving the details about a new SP, the user who requested to register it becomes its first SP administrator. An SP administrator can transfer the administration right to further users. Only users with administrator rights for a specific SP are able to modify its elements and attributes. Such changes require re-approval by an RRA Administrator.

Additional Rules for Federation Partner Service Providers

A signed Federation Partner Agreement is required before a Federation Partner SP can register with the federation. Federation Partner SPs are always approved by a Federation Operator.

Practices regarding metadata modifications

In eduID, no metadata gets modified because the federation operator generates it on behalf of all entities.

The source for generating metadata is the Resource Registry. The details of a registering entity are entered manually by providing the necessary information. Alternatively, a wizard will parse existing entity metadata to gather as many details as possible in order to facilitate the registration.

The IdP/SP administrator also has to supply non-technical information like descriptions or support contacts. All technical and non-technical information is stored as decomposed items in a database.

To generate federation metadata, information from that database gets composed into SAML metadata format.

All entites in the Resource Registry could be in one or more metadata-sets. Beside the federation metadata there are metadata-sets with generated metadata files for each institution and for edugain.

---

[1] RRA Administrator = Resource Registration Authority Administrator A role assigned to one or more persons to act on behalf of the institution which signed the federation service agreement. An RRA Administrator has to review and approve new and changed SPs belonging to or sponsored by the institution before such an SP gets loaded into federation metadata.

HREF metadata specifikáció

A föderációs metaadat célja, hogy a föderációban részt vevő intézmények illetve entitások technikai, bizalmi és adminisztratív adatait egy helyre gyűjtse. A metaadatok formátuma megfelel a SAML2 metaadat szabványnak.

Biztonsági megfontolások

Mivel a metadata tartalmazza a föderációban részt vevő tagok és komponensek technikai információit, ezért a benne tárolt információkkal kapcsolatban figyelembe kell venni a következő biztonsági megfontolásokat:

- Téves vagy kompromittálódott adatok eltávolítása esetén a sérülékenységi ablak megegyezik a metadata gyorstárazhatósági (`cacheDuration`) idejével, **amennyiben a támadó nem képes blokkolni a központi metaadatok elérhetőségét (DOS)**
- Amennyiben a támadó képes blokkolni a központi metaadatok elérhetőségét, a sérülékenységi ablak a legutolsó letöltött metadata állomány érvényességéig (`validUntil` paraméterében meghatározott ideig) tart.
- Amennyiben a metaadatok érvényességi ideje lejár, az entitás nem képes azonosítani a többi föderációs résztvevőt, ezért nem tud föderációs szolgáltatást (pl. IdP esetén azonosítási szolgáltatást) nyújtani.

Metaadatban tárolt információk

- Bizalom a metaadatban
  - a metaadat integritásvédelmét és hitelességét egy digitális aláírás biztosítja.
  - a metaadat visszavonhatóságát a lejárati idő (`validUntil`) biztosítja, ami jelenleg 3 nap.
  - az egyes rendszerek gyorstárazhatják a metaadatot, de legalább naponta egyszer kötelesek a hiteles állományt frissíteni.
  - az aláírási procedúrát a Metaadat_aláírásának_módja fejezet írja le.
- Tanúsítványok
  - kötelező legalább 1024 bites kulcspárt használni
  - az entitások által használt tanúsítvánnyal kapcsolatban a föderáció nem tesz különleges megkötést, sőt: ajánlott hosszú lejáratú self-signed tanúsítványok használata
- További információk
  - minden szöveges mezőt legalább két nyelven: magyarul és angolul ki kell tölteni

- kötelezően kitöltendőek az intézményi, adminisztratív információk (`Organization` illetve `ContactPerson` elemek)
- ajánlott megadni egy helpdesk URL-r, ahova hiba esetén a felhasználók fordulhatnak (`errorURL` attribútum)
- SP-k esetén további kötelező elemek
  - `AttributeConsumingService`, ami megadja a kért attribútumokat
    - `RequestedAttributes` - itt az attribútum informális neve is szerepeljen
    - `ServiceName`, `ServiceDescription` az SP szolgáltatás neve és leírása
  - a szolgáltatás elérhetősége, amin a szolgáltatás bemutatkozik (extension)
  - adatkezelési szabályzatra mutató URL (extension)
- IdP-k esetén
  - a scope csak az adott intézmény kezelésében levő domain név lehet (Shibboleth extension)
- lehetőség van további adatok megadására is
  - logó
  - gps koordináták, IP cím tartomány
  - különböző tagek, például a szolgáltatás publikus-e, vagy épp bevezetés alatt áll-e

Metaadat kiterjesztések használata

Ezen kiegészítő adatok tárolására az internet2 szabványtervezetet készít, ennek a sémának a jelenlegi verziója megtalálható itt.

A kiegészítő séma névtere: `urn:oasis:names:tc:SAML:2.0:metadata:ui`. Az alábbi táblázatban ezen névtérben definiált legfontosabb elemeket foglaljuk össze:

element név	szemantika	értékekre vonatkozó megkötések
GeolocationHint	szélesség és hosszúság érték, a + előjel az északi szélességet illetve keleti hosszúságot jelöli	47.47359,19.052891
InformationURL	az entitásról további információkat (pl. helpdesk) szolgáltató oldal.	
PrivacyStatementURL	Az SP adatvédelmi nyilatkozátnak elérhetősége (URL)	Engedélyezett formátumok: HTML, PDF
Logo	Az IdP/SP logójának elérhetősége	Formátummal kapcsolatban lásd Logo
IPHint	(Csak az IdP-knél) az intézmény hálózati tartománya(i). IdP felderítés esetén előválasztás lehetséges ennek alapján.	CIDR, több érték is megadható
DomainHint	(Csak az IdP-knél) az intézmény által felügyelt domain név. IdP felderítés esetén előválasztás lehetséges ennek alapján.	Több érték is megadható

Logo

- formátum: URL egy transzparens hátterű PNG, vagy transzparens hátterű GIF képre
- méretezés
  - javasolt oldalarány 1:1 vagy 16:9
  - maximális méret 200x200px
  - ajánlott egy 16x16px-es verziót is megadni
- attribútumok
  - `xml:lang`: lokalizációs információ
  - `href`: opcionális link
  - `height`: opcionális magasság érték pixelben
  - `width`: opcionális szélesség érték pixelben

Egy IdP példa

```
 <EntityDescriptor entityID="https://idp.niif.hu/shibboleth"
  xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">
   <Extensions>
    <shibmd:Scope>niif.hu</shibmd:Scope>
    <mdui:DiscoHints xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <mdui:GeolocationHint>47.518356,19.055437</mdui:GeolocationHint>
      <mdui:DomainHint>niif.hu</mdui:DomainHint>
      <mdui:DomainHint>iif.hu</mdui:DomainHint>
    </mdui:DiscoHints>
   </Extensions>
   <KeyDescriptor use="signing">
    <ds:KeyInfo>
     <ds:X509Data>
      <ds:X509Certificate>...</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </KeyDescriptor>
   <!-- endpoints, nameidformats -->
   </IDPSSODescriptor>
  <ContactPerson contactType="technical">
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="support">
```

```
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="administrative">
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
 </EntityDescriptor>
```

Egy SP példa

```
 <EntityDescriptor entityID="https://rr.aai.niif.hu/shibboleth"
  xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">
 <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
  <Extensions>
    <mdui:UIInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <mdui:PrivacyStatementURL>https://rr.aai.niif.hu/privacy-
policy</mdui:PrivacyStatementURL>
      <mdui:InformationURL>https://rr.aai.niif.hu/about</mdui:InformationURL>
    </mdui:UIInfo>
  </Extensions>
  <KeyDescriptor use="signing">
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>...</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </KeyDescriptor>
  <KeyDescriptor use="encryption">
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>...</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </KeyDescriptor>
  <!-- endpoints -->
  <AttributeConsumingService index="1">
   <ServiceName xml:lang="hu">HREF Resource Registry</ServiceName>
```

```
   <ServiceName xml:lang="en">HREF Resource Registry</ServiceName>
   <ServiceDescription xml:lang="hu">Resource Registry - a föderáció adminisztrációs
alkalmazása http://rr.aai.niif.hu/</ServiceDescription>
   <ServiceDescription xml:lang="en">Resource Registry - federation administration tool
http://rr.aai.niif.hu/</ServiceDescription>
   <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
isRequired="true"/>
   <RequestedAttribute FriendlyName="surname" Name="urn:oid:2.5.4.4" isRequired="true"/>
   <RequestedAttribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" isRequired="true"/>
   <RequestedAttribute FriendlyName="eduPersonPrincipalName"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" isRequired="true"/>
   <RequestedAttribute FriendlyName="schacHomeOrganizationType"
Name="urn:oid:1.3.6.1.4.1.25178.1.2.10" isRequired="true"/>
   <RequestedAttribute FriendlyName="eduPersonScopedAffiliation"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" isRequired="true"/>
  </AttributeConsumingService>
 </SPSSODescriptor>
 <Organization>
  <OrganizationName xml:lang="hu">NIIF - Nemzeti Információs Infrastruktúra Fejlesztési
Intézet</OrganizationName>
  <OrganizationName xml:lang="en">NIIF Institute - National Information Infrastructure
Development</OrganizationName>
  <OrganizationDisplayName xml:lang="hu">NIIF - Nemzeti Információs Infrastruktúra Fejlesztési
Intézet</OrganizationDisplayName>
  <OrganizationDisplayName xml:lang="en">NIIF Institute - National Information Infrastructure
Development</OrganizationDisplayName>
  <OrganizationURL xml:lang="hu">http://www.niif.hu</OrganizationURL>
  <OrganizationURL xml:lang="en">http://www.niif.hu/en</OrganizationURL>
 </Organization>
 <ContactPerson contactType="administrative">
  <SurName>NIIF AAI</SurName>
  <EmailAddress>aai@niif.hu</EmailAddress>
 </ContactPerson>
 <ContactPerson contactType="technical">
  <SurName>NIIF AAI</SurName>
  <EmailAddress>aai@niif.hu</EmailAddress>
 </ContactPerson>
 <ContactPerson contactType="support">
  <SurName>NIIF AAI</SurName>
```

```
  <EmailAddress>aai@niif.hu</EmailAddress>
</ContactPerson>
</EntityDescriptor>
```

Metaadat aláírásának módja

Aláíró kulcs és tanúsítványok

HREF-2011

- Az aláíró kulcsot smart cardon, pin kóddal védve tároljuk.
- Az aláírás on-line történik, a kártya pin kódját az aláíró szoftver indításakor az AAI adminisztrátor adja meg, a jelszó nem kerül tárolásra az aláírást végző rendszeren (sem másutt).

HREF-2020

- 4096 bites, SHA-384 RSA aláíró kulcs.
- Az aláírás on-line történik, több telephelyes tartalékolt infrastruktúrával.

Aláírási folyamat

Az aláíratlan metaadat frissítése:

1. Az aláíratlan metaadat a https://rr.eduid.hu oldalról ütemezetten, minden óra 15. és 45. percében letöltésre kerül.
2. A letöltött metaadat XML séma ellenőrzése ellenőrzése.
3. A metadat feltöltése az objektum tárolóba.

Aláírás ellen?rzése explicit tanúsítvánnyal

A föderáció entitásai a föderációs metaadat hitelességéről a digitális aláírás ellenőrzésével győződhetnek meg. Az explicit ellenőrzés esetén a `[http://metadata.eduid.hu/current/](http://metadata.eduid.hu/current/)` URL-ről kell letölteni a metadata fájlokat.

Ajánlott a tanúsítvány lejárati idejét figyelmen kívül hagyni.

HREF-2011

- A HREF-2011 tanúsítvány a https://metadata.eduid.hu oldalról érhető el.

SHA-1	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
Serial Number	1
Version	3
C	HU
O	NIIF Institute
OU	eduID Federation Operator
CN	Metadata Signer
emailAddress	aai@niif.hu
Érvényesség kezdete	2011.10.05.
Érvényesség vége	2031.09.30.

HREF-2020

- A HREF-2020 tanúsítvány a https://metadata.eduid.hu oldalról érhető el.

SHA-1	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`
Serial Number	80:21:EF:F0:BA:16:04:BD
Version	1
C	HU
ST	Budapest
L	Budapest
O	Governmental Agency for IT Development
OU	eduID Federation Operator
CN	Metadata Signer
emailAddress	info@eduid.hu
Érvényesség kezdete	2020.06.13.
Érvényesség vége	2025.06.14.

Aláíró kulcs cseréje

- A kulccsere koordinálása a `href-tech` levelezőlistán keresztül történik.
- Kulcs visszavonásakor (kompromittálódás gyanúja esetén) a régi aláíró kulcs azonnal eltávolításra kerül, kontrollált kulcscsere esetén az aláírás párhuzamosan történik a régi és az új kulccsal.

Metaadat elérése

A HREF föderációban többféle metaadat-forrás áll rendelkezésre, melyeket a http://metadata.eduid.hu -ról lehet elérni. Fontos megemlíteni, hogy a metadata letöltésénél nem indokolt az SSL használata, ezért - amennyiben lehetséges -, érdemes a metadata URL-eket nem titkosított HTTP protokoll segítségével letölteni.

A metadata elérés URL-je a következő:
`http://metadata.eduid.hu/${alairo_kulcs_kibocsatas_eve}/${metadata_forras}.xml`.

A metadata források jelenleg a következők lehetnek:

`href.xml`	**Az éles föderációban részt vevő, és a föderáció kritériumait teljesítő entitások.**
`href-test.xml`	A HREF föderáció tesztrendszerei. Bármely, a föderációban részt vevő intézmény tehet be teszt-entitást ebbe a halmazba, ezért ezen metaadat-forrás csak tesztelési célra használható.
`href-pending.xml`	A HREF föderáció "előszobája". Az újonnan csatlakozó intézmények IdP-je először itt lesz elérhető.
`href-edugain.xml`	A HREF föderációból az eduGAIN konföderációba kiajánlott entitások. Ide csak olyan entitások kerülhetnek be, melyek megfelelnek a föderációs kritériumoknak, és képesek az eduGAIN konföderációval való együttműködésre. Ezen entitások be kell hogy olvassák az eduGAIN metaadatot is.
`edugain.xml`	Az eduGAIN konföderáció metaadata, a HREF aláíró kulccsal aláírva.
`intézmény-specifikus`	Az intézmény-specifikus metaadat fájlok (pl.: bme.xml, ceu.xml, stb.), melyeket a föderáció kérésre biztosítja, tetszőleges entitások halmazba gyűjtésével.

MDX-alapú elérés

Az MDX, azaz MetaDataeXchange protokolt erőforrás optimalizálás céljából találták ki, hogy ne kelljen egyes IdP-knek és SP-knek indokolatlanul nagy XML fájlokat feldolgozniuk és tárolniuk, mikor a felhasználóiknak jó eséllyel a fájlokban tárolt entitások töredékére van csak szükségük. Ezért az egyes entitásokat be lehet úgy állítani, hogy csak akkor töltsék le az adott entitás metaadatát, mikor arra szükség van (az első letöltés után természetesen helyben tároldóik a metaadat a `cacheDuration`-ben megadott ideig).

A HREF föderációban teszt jelleggel működik és elérhető MDX-kiszolgáló: http://mdx.eduid.hu. A megfelelő beállításokhoz itt érhető el segédlet.

Az MDX kiszolgáló eltérő kulcsot és tanúsítványt használ. Jelenleg az MDX elérés még csak teszt jelleggel működik, az élesüzemre váltáskor a HREF-2020 tanúsítvánnyal fog működni.

A jelenlegi tanúsítvány innen tölthető le: http://metadata.eduid.hu/current/mdx-test-signer-2015.crt

HREF-2015

SHA-1	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
Serial Number	AA:90:7C:D9:0C:D5:64:8D
Version	3
C	HU
ST	-
L	Budapest
O	NIIFI
OU	AAI
CN	eduID MDX metadata signer
emailAddress	aai@niif.hu
Érvényesség kezdete	2015.10.13.
Érvényesség vége	2034.12.12.

FederationStats

Federation usage statistics

!!! warning "A szócikk vagy fejezet még megírásra vár"

```
I am a stub, please fix me!
```

Federation visualization project - discountinued.

- source (ruby on rails) https://repo.niif.hu/gitweb/gitweb.cgi?p=federation-stats.git;a=summary
- live demo

Running the sample project

- Install Ruby
- Install Rails (`gem install rails`)
- Setup a `development.sqlite3` database with the `rake db:setup` command
- Fire up `script/server`, it will run the project on localhost:3000

Statistic types

Currently we have the following types of statistics:

- Unique users per day (`USER_COUNT`)
- AuthnResponse per day (`AUTH`)
- AuthnResponse per service per day (`SSO_TO_SERVICE`)

Log statistics format

The following simple format is used to convey statistics from IdPs to the central module - the white spaces (new lines) are important:

```
ENTITYID #ENTITYID#
APIKEY #API_KEY#
DATE yyyy-mm-dd

STAT #STAT_ID#
xxxx

STAT #STAT_ID#
yyyy

STAT #STAT_ID#
ww | #PEER_ENTITY_1#
zz | #PEER_ENTITY_2#
```

The following sample might help understanding the format:

```
ENTITYID https://idp.niif.hu/idp/shibboleth
APIKEY 0123.......
DATE 2009-03-18

STAT AUTH
68 logins

STAT USER_COUNT
16 unique userids

STAT SSO_TO_SERVICE
1        | urn:geant:niif.hu:niifi:sp:register.ca.niif.hu
12       | https://repo.niif.hu/shibboleth
1        | https://sandbox.aai.niif.hu/shibboleth
5        | https://sysmonitor.hbone.hu/shibboleth
10       | https://www.ki.iif.hu/shibboleth
1        | https://noc6.vh.hbone.hu/shibboleth
21       | https://webadmin.iif.hu/shibboleth
3        | https://rrd-ma.perfsonar.vh.hbone.hu/shibboleth
7        | https://ugyeletes.vh.hbone.hu/shibboleth
2        | https://noc.grid.niif.hu/shibboleth
1        | https://wiki.voip.niif.hu/shibboleth
2        | https://netmonitor.hbone.hu/shibboleth
2        | https://idp.sch.bme.hu:443/opensso/sp/test
```

Running the log statistics collector

This following script can be used the collect statistics from the idp audit logs of Shibboleth 2 IdP generated on the day before running. It is based on Peter Schober's audit_r7.py, and good for run from daily cronjob:

```
#!/bin/bash

#Config section
PARSER_COMMAND="/opt/shibboleth-idp/bin/audit_r7.py"
SOURCEDIR="/opt/shibboleth-idp/logs"
TARGETDIR="/tmp"

ENTITYID="idp-entity-id"
APIKEY="aaa..."
LOCATION2PUT="https://fedstats.example.org/import_stats"

DATE=`date -d "yesterday" +"%Y-%m-%d"`
SOURCEFILE="$SOURCEDIR/idp-audit-$DATE.log"

#Should not edit below this

if [-f $SOURCEFILE ]()
then
    LOGINS=`$PARSER_COMMAND -l $SOURCEFILE`
    UNIQUE_LOGINS=`$PARSER_COMMAND -u $SOURCEFILE`
    SERVICES=`$PARSER_COMMAND -p $SOURCEFILE | sed '/^[0-9]/p' -n`

    TARGETFILE="stat-$DATE.log"

echo "ENTITYID $ENTITYID
APIKEY $APIKEY
DATE $DATE

STAT AUTH
$LOGINS

STAT USER_COUNT
$UNIQUE_LOGINS
```

```
STAT SSO_TO_SERVICE
$SERVICES
" > $TARGETDIR/$TARGETFILE

    wget -q --no-check-certificate --post-file=$TARGETDIR/$TARGETFILE $LOCATION2PUT -O
/dev/null
    rm $TARGETDIR/$TARGETFILE
fi
```

The script below can be used the collect statistics from all the idp audit logs placed in a folder.

```
#!/bin/bash

#Config section
PARSER_COMMAND="/opt/shibboleth-idp/bin/audit_r7.py"
SOURCEDIR="/opt/shibboleth-idp/logs"
TARGETDIR="/tmp"

ENTITYID="idp-entity-id"
APIKEY="aaa..."
LOCATION2PUT="https://fedstats.example.org/import_stats"

FILES="idp-audit-*.log"

#Should not edit below this
cd $SOURCEDIR
for f in $FILES
do
  if [-f $f ]()
  then
    echo "Processing $f file..."
    DATE=${f:10:10}
    LOGINS=`$PARSER_COMMAND -l $f`
    UNIQUE_LOGINS=`$PARSER_COMMAND -u $f`
    SERVICES=`$PARSER_COMMAND -p $f | sed '/^[0-9]/p' -n`

    TARGETFILE="stat-$DATE.log"

    echo "ENTITYID $ENTITYID
```

```
APIKEY $APIKEY
DATE $DATE

STAT AUTH
$LOGINS

STAT USER_COUNT
$UNIQUE_LOGINS

STAT SSO_TO_SERVICE
$SERVICES
" > $TARGETDIR/$TARGETFILE

    wget -q --no-check-certificate --post-file=$TARGETDIR/$TARGETFILE $LOCATION2PUT -O
/dev/null
    rm $TARGETDIR/$TARGETFILE
  fi
done
```

Feeding the database with the statistics

The federation statistics rails project contains the `script/stat_parser/file.rb` command which can process the statistics format and load the data to the database. Note that this script currently contains an absolute path for the `script/runner` script, so you must fix this before use.

Using HTTP-Post to feed the database

When deployed, the rails project provides a `/import_stats` URL to which one could POST the generated statistics file.

Creating IdPs

Use the rails console to create new idps:

```
$ RAILS_ENV=production script/console

>> Entity.create :name => 'foo', :entity_type => 'idp'
```

```
=> #<Entity id: 1, name: "foo", entity_type: "idp", created_at: "2010-11-29 14:55:40",
updated_at: "2010-11-29 14:55:40", api_key: "da9l233a45698fa5c4a252e301e3da2sf5ece24e">
```

HREFGlossary

Föderáció

Olyan bizalmi szövetség, melynek résztvevői elfogadják egymás felhasználóit azonosítottnak.

HREF Föderáció

(Hungarian Research and Education Federation, Magyar Kutatási és Felsőoktatási Föderáció), magyar felsőoktatási, kutatási intézmények és közgyűjtemények föderációja.

Föderációs Operátor

A Föderációs Operátor a Tagokkal és Partnerekkel megkötött csatlakozási szerződés alapján a HREF föderáció központi szolgáltatásainak működtetője. Elsődleges szerepe az, hogy a tagok közötti bizalmi viszonyt kialakítsa és fenntartsa.

Gyakorlati feladatai közé tartozik a központi szolgáltatások működtetése (Discovery Service, Resource Registry), a Metadata állomány karbantartása és rendszeres aláírása, valamint a tagokkal ill. partnerekkel való szerződéses viszony kialakítása. A Föderációs Operátor vállalt feladatait és ezek szolgáltatási szint paramétereit az SLA megállapodás tartalmazza.

Felhasználó

Egy Tag alkalmazottja, oktatási tevékenységet végző munkatársa ill. hallgatója, akik igénybevehetik a Tartalomszolgáltatók szolgáltatásait.

Tag

A HREF Föderációhoz a Föderációs Operátorral megkötött csatlakozási szerződés alapján csatlakozó intézmény. Ilyen módon csak magyar felsőoktatási, kutatási, ill. oktatási és közgyűjteményi tevékenységet folytató jogi személyek csatlakozhatnak.

A Tag azonosított felhasználói igénybe vehenek más tagok ill. Partnerek által biztosított szolgáltatásokat.

Partner

A HREF Föderációhoz a Föderációs Operátorral megkötött csatlakozási szerződés alapján csatlakozó partner intézmény.

Partner intézmény szolgáltatásokat biztosíthat Tagok által azonosított felhasználók számára.

Tagok Tanácsa

A Föderáció működését szabályozó dokumentumokat a Föderációs Operátor a Tagok Tanácsa jóváhagyásával módosíthatja.

IdP

Identity Provider. Szövegkörnyezettől függően jelentheti az Azonosító Szervezetet, ill. az IdP AAI Kaput.

Azonosító Szervezet

A felhasználók azonosítását elvégző intézmény ("saját intézmény"). Az azonosító szervezet - az adatvédelmi szabályok betartása mellett - a felhasználóról Attribútumokat adhat át a Tartalomszolgáltatónak

Attribútum

A felhasználóhoz kapcsolódó személyes adat, illetve a felhasználó intézményhez való viszonyát leíró adat. A felhasználó attribútumait az Azonosító Szervezet tartja karban. Az attribútumok egy jól meghatározott halmazát az azonosítási folyamat részeként az IdP AAI Kapu átadja a Tartalomszolgáltatónak.

IdP AAI Kapu

Az a szoftver, amely elvégzi a felhasználók azonosítását és lehetőséget biztosít az azonosítással kapcsolatos információk, valamint felhasználói adatok (Attribútumok) kiadására.

SP

Service Provider. Szövegkörnyezettől függően jelentheti a Tartalomszolgáltatót, ill. az SP AAI Kaput.

Tartalomszolgáltató

A Tartalomszolgáltató az Azonosító Szervezet azonosítása alapján, az arra jogosult felhasználók számára webes szolgáltatásokat nyújtó szervezet. A HREF Föderációban Tartalomszolgáltatóként részt vehet mind a Tag, mind a Partner.

SP AAI Kapu

Az a szoftver, amely értelmezi az Azonosító Szervezettől kapott adatokat, ellenőrzi a kapott üzenet az érvényességét és sértetlenségét, majd jogosultságellenőrzést végez.

Entitás

Az SP AAI Kapu és az IdP AAI Kapu összefoglaló neve.

Saját SP

Tag által üzemeltett webes szolgáltatás, amely kizárólag intézményen belül elérhető. Saját SP-k regisztrálhatók a Resource Registry segítségével, azonban a föderációs metadatában nem jelennek meg.

Resource Registry

A Resource Registry az HREF Föderáció működtetéséhez szükséges olyan nyilvántartás, amely az Azonosító Szervezetekre és a Tartalomszolgáltatókra vonatkozó információkat kezeli. A Resource Registry segítségével előállítható és szerkeszthető a föderációs Metadata, valamint az Azonosító Szervezetek által a Tartalomszolgáltatók részére átadandó információkra vonatkozó szabályok.

Discovery Service

A Föderációs Operátor által üzemeltetett Keresőszolgáltatás (Discovery Service) egy olyan webes felület, ahol a felhasználók kiválaszthatják az őket azonosítani tudó Azonosító Szervezetet.

Keresőszolgáltatást Tartalomszolgáltató és Azonosító Szervezet is üzemeltethet.

Metaadatok

(Metadata) Az HREF Föderációban résztvevő intézményeket leíró adatállomány. Az állomány tartalmaz:

- technikai információkat
- kontaktok elérhetőségi adatokat
- leíró adatokat Az állományban található adatokat, valamint az állomány kezelésével kapcsolatos előírásokat a Metadata Specifikáció részletezi.

Virtuális Azonosító Szervezet

(VHO, Virtual Home Organization) A Föderációs Operátor által üzemeltetett szolgáltatás, mely azonosítási szolgáltatást nyújt a Föderációban Tagként nem szereplő intézmények felhasználói számára, illetve lehetőséget biztosít a Tagok vendég felhasználói adminisztrálására is.

URN

Registrations in the urn:geant:niif.hu Namespace

GEANT has delegated the operation of urn:geant:niif.hu namespace to NIIFI -> KIFÜ. KIFÜ administers the Uniform Resource Name namespace urn:geant:niif.hu, which enables all scientific institutions in Hungary to assign unique, permanent and globally valid names to different resources. The exact use of the entries is not prescribed. GÉANT primarily wants to promote standardization within the scientific community and especially the interoperability of middleware with the namespace.

If you want to request a delegation, please send an email to urn@niif.hu.

Namespaces administered by KIFÜ

Namespace	Purpose	Date Registered	Registry link/email
urn:geant:niif.hu:niif	Namespace supporting KIFÜ systems	10 March 2010	urn@niif.hu
-	-	-	-

URN SCHAC

URN schac sémák

URN Registry

Géant névtér

A Dante regisztrált egy önálló namespace-t a Géant számára `urn:geant` néven. Ezt a namespace-et közvetlenül a Dante felügyeli.

A regisztrált névterek listája itt tekinthető meg.

URN Registry Application

A RedIris kifejlesztett egy URN névtér kezelő alkalmazást, amelyben definiálni lehet az egyes URN-ek jelentését.

Az URNReg alkalmazás itt érhető el.

Függ?ségek

- Apache (kipróbálva: 2.2.3)
- PHP (kipróbálva: 5.2.0)
- LDAP szerver (kipróbálva: slapd 2.3.30)
- SiLeDAP (kipróbálva: 0.2)

Slapd inicializálás

A Quickstart Guide alapján **SEM** kell megtenni, mert a Debian telepítő elintézi helyettünk.

Schema

Be kell másolni a kicsomagolt program alatt a `schemata/urnReg.schema` a `/etc/ldap/schema/` könyvtárba, és a `/etc/ldap/slapd.conf` -ban include-olni kell.

- **BUG1**: A schema állományból töröljük az `sn1` és `sn2` attribútumokra való hivatkozásokat!

SiLeDAP

Fogalmam sincs, mit csinál ez a függőség. A leírás szerint így kell telepíteni:

```
mkdir siLeDAP
cd siLeDAP
tar xzvf /tmp/siledap-api-0.2.tar.gz
```

- **BUG2**: a tar.gz tele van ._Ldap kezdetű állományokkal. Ezeket törölni kell.

Be kell állítani az LDAP kapcsolat paramétereit az `LdapConf.php` állományban. A file tartalmaz egy HTTP_BASE változót, arra nem lesz szükség, kommenteljük ki.

simpleSAMLphp

Konfiguráció

config.php

browser/js/URNregConfig.js