NIIF INTÉZET – HBONE+ PROGRAM
H–1132 Budapest, Victor Hugo utca 18–22. · postacím: H–1396 Budapest 62, Pf. 498.
telefon: (1) 450-3060 · fax: (1) 350-6750 · e-mail: info@hboneplus.hu · url: www.hboneplus.hu

KMOP-4.2.1/A_2-08/1-2009-0001 és TIOP-1.3.2-08/1-2009-0001

HBONE+

felsőoktatási információs infrastruktúra fejlesztése

EMLÉKEZTETŐ

MELLÉKLET A MAGYAR KUTATÁSI ÉS FELSŐOKTATÁSI FÖDERÁCIÓ (HREF) KERETÉBEN TÖRTÉNŐ ADATKEZELÉSSEL KAPCSOLATOS ÁLLÁSFOGLALÁSHOZ

Dátum: 2009.09.29.	***Revizió***	1.0
Minősítése: nyilvános		

TARTALOMJEGYZÉK

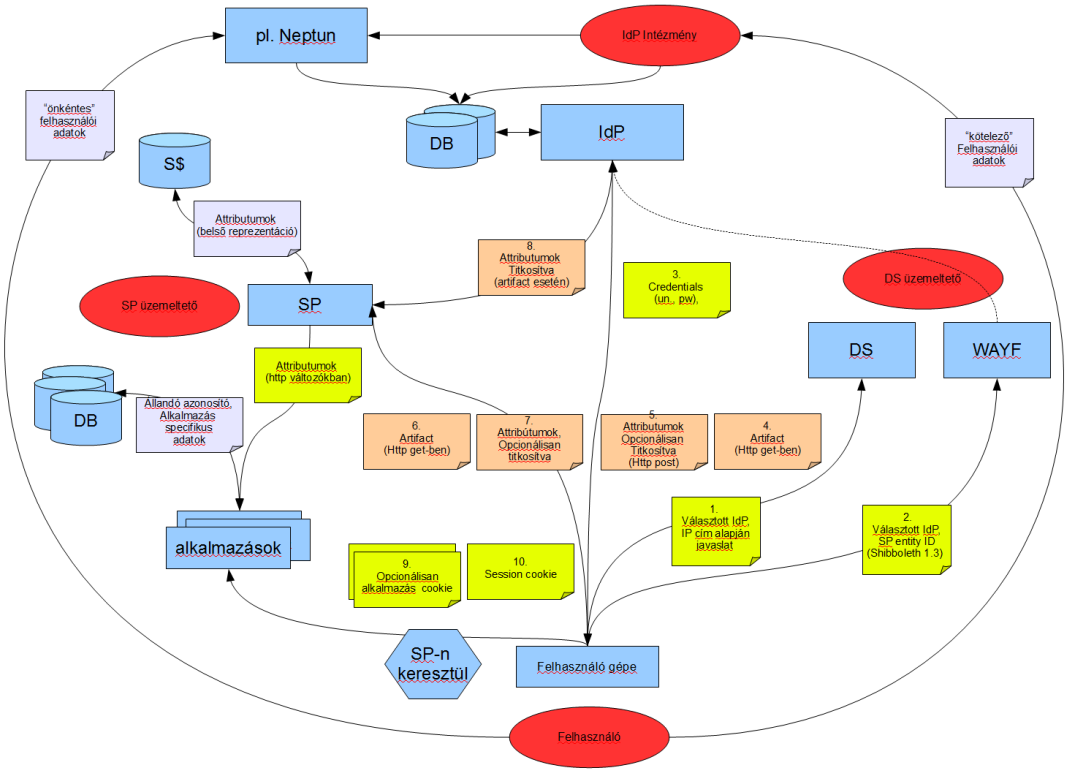
Jelen emlékeztető célja, hogy összefoglalja a Magyar Kutatási és Felsőoktatási Föderációnak (HREF) az adatvédelmi előírásoknak való megfelelőségével kapcsolatos, 2009.05.12. - 2009.09.30. között megtartott megbeszéléseken elhangzottakat.

1 Áttekintés

1.1 Magyar Kutatási és Felsőoktatási Föderáció (HREF)

A NIIF AAI projektben a HREF föderáció körébe tartozó - jelenleg 5 intézmény - közötti azonosítási és hitelesítési kommunikációt a Shibboleth nevű alkalmazás valósítja meg, ami Single Sign-On vagyis egyszeri bejelentkezést és központi felhasználó és/vagy jogosultság menedzsmentet tesz lehetővé. A Shibboleth egy elosztott azonosítási és hitelesítése rendszer, ahol az erőforrásokhoz történő hozzáférés az identitás-szolgáltatótól kapott attribútumok alapján történik. Az egyes felhasználók úgy vehetik igénybe a szolgáltatásokat a föderáción belül, hogy csak egyetlen identitással rendelkeznek a saját „anyaintézményüknél” (home institution).

A Shibboleth alapú föderációk esetében a felhasználói azonosítás és jogosultságkezelés a SAML XML üzenetek továbbításával történik, mely üzeneteket a Shibboleth további alkotóelemei továbbítják az érintett felek között.



1. ábra

A fenti ábra (1. ábra) felvázolja a föderációban résztvevő intézménytípusok, valamint a felhasználók és más entitások között létrejövő adatforgalom alapvető struktúráját, továbbá az adatforgalom és a szereplők között továbbított adatok típusát.

2 Föderációban használt alkalmazások

2.1 IdP és SP funkciókra

1. Támogatott alkalmazások
    - Shibboleth
    - Simple SAML PhP
2. Tetszőleges SAML 2 képes alkalmazások
3. VHO tools (felhasználói adminisztrációs alkalmazás, a föderáció más tagjai is fel tudnak venni a felhasználókat a VHO-ba)

2.2 Föderációs központi "adminisztrációs" alkalmazások

1. Discovery Service
    - Switch
    - Internet2
    - más egyéb megoldás (pl. SP-be beágyazott megoldás)
2. WAYF szolgáltatások (valószínűleg nem fogja senki sem használni)
3. Resource Registry (generálni tudja a metadata-t, Attribute Filter-t (IdP oldali), Attribute Policy-t (SP oldali)

2.3 Alkalmazás elemek funkciói

2.3.1 Identity Provider (IdP) – Identitás szolgáltató (home organization)

Az IdP-t üzemeltető „anyaintézmény” általában az alábbi típusú adatokat tárolja a felhasználókról az azonosításhoz:

1. kötelezően megadandó adatok (kifejezetten a föderáció működéséhez bekért adatok)
2. önkéntesen megadott adatok (pl. felhasználóról készült fotók, mobil telefonszám)

Az intézmény általában valamilyen címtár vagy felhasználói adatbázisból kapja meg az azonosításhoz szükséges adatokat.

2.3.2 Service Provider (SP) – Szolgáltatásnyújtó

A Shibboleth alkalmazás szerint az egyes IdP-k és SP-k egymás megbízható partnerei (relying party), vagyis az IdP számára az alkalmazás adta lehetőség szerint relying party az SP és fordítva. Az egyes intézmények és szolgáltatók számára az EntityID az az egyedi azonosító, amivel egymást azonosítani képesek. Az IdP és SP HTTP azonosító címeket (URL-eket) használ egyedi azonosítóként.

Az IdP-k és SP-k tanúsítványa a metadatában van beleágyazva (self-signed).

2.3.3 Discovery Service (DS) - Azonosító szervezet

A DS feladata technikai jellegű, amely alapján közli az SP-vel, hogy a felhasználónak ki az IdP-je. Korábban „Where are you from?” (WAYF) szolgáltatás látta el ezt a funkciót.[1]

A DS a WAYF-tól abban különbözik, hogy a WAYF nem az SP-nek mondja meg az információt, hanem megkapja az SP-től teljes autentikációs kérést és továbbítja az IdP-nek és ebben az esetben nem megy át az autentikációs kérés a DS-en, hanem a felhasználó választja ki egy felületen, hogy ki az IdP, aki azonosítani fogja. A DS megpróbálhatja kitalálni (valós időben megtippelni) az IdP-t IP cím alapján (majd a

[1] Megjegyzendő, hogy noha lehetőség marad a SAML ezen korábbi verziójával kompatibilis WAYF szolgáltatás alkalmazására (Shibboleth 1.3 esetében), azonban SAML 2 kompatibilis SP-k számára a DS használata javasolt.

felhasználó választását egy cookie-ban képes eltárolni). Fontos megjegyezni, hogy mindig az SP választ DS-t.

A DS üzemeltetését a Föderáció fogja végezni, itt meg kell lennie minden IdP-nek. A DS üzemeltetése kritikus kérdés, technikailag nem kötelező, hogy egy darab DS legyen, így nem kizárt, hogy a föderációban benne lévő más intézmények is üzemeltessenek DS-t, célszerű azonban, hogy bárki is az üzemeltető, a DS-t a metadat alapján üzemeltessék. Az intézmények érdekeltek lehetnek abban, hogy DS-t üzemeltessenek, hiszen ebben az esetben az adott intézmény határozza meg, hogy milyen IdP-ket, SP-ket jelenít meg, vagy olyan IdP-t akar megjeleníteni, aki nem tagja a föderációnak.

2.3.4 OpenSAML C++ and Java könyvtárak

A SAML üzenet formátumokat határoz meg, amelyek lehetnek (1) protokollok és (2) assertion-ök (assertion=struktúra) (együtt: SAML2.0 core), (3) binding-ok (XML üzenetek eljuttatása egyik pontból a másikba; pl. HTTP POST binding, artifact) és (4) profile-okat (alkalmazási területek követelményrendszerei, leírásai; pl. single sign on).

A Shibboleth SAML profile-okat valósít meg, a SAML üzenetek előállítására az alkalmazás a OpenSAML-t használja. Az Open SAML a binding-okat, a protokollokat és a SAML assertion-öket implementálja (pl. assertion query). Open SAML közvetlenül nem kérdez le adatokat, azokat nem módosítja, mivel mindet készen kap.

2.3.5 Virtual Home Organization (VHO)

Virtuális azonosító szervezet gyakorlatilag egy IdP, vagyis ugyanazokat a funkciókat látja el, mint egy IdP. A VHO célja, hogy olyan személyek számára is lehetőséget biztosítson föderációban történő részvételre, így azonosításra, amelyek egyéni felhasználók vagy az anyaintézményük nem tagja a föderációnak, tehát nem IdP-k. A NIIF a virtuális azonosító szervezet, mint egyfajta központi IdP szervezet feladatait egy outsourcing szolgáltatásként kívánja nyújtani.

2.3.6 Resource Registry

A Resource Registry egy olyan keretrendszer, amely az új IdP-k és SP-k regisztrálására és a meglévők entitások módosítására alkalmas. A már regisztrált IdP-kből és Sp-kből állítja elő azt a SAML 2 metadata fájlt, amit mindenki le tud tölteni. Másodlagos szerepe, hogy az IdP-k megadhatják, hogy milyen attribútumokat

támogatnak, az SP-k pedig megadhatják, hogy milyen attribútumokat követelnek meg, használnak. Az AttributeFilter és az AttributePolicy előállításához egy webes felületet ad, amelyen keresztül Shibboleth konfiguráció elvégezhető. A Resource Registry nyújt segítséget az intézmény adminisztrátorának, hogy kivel működjön együtt. A HREF-ben jelenleg a SWITCH svájci föderáció által kifejlesztett Resource Registry-t alkalmazzák.

3 Föderáció szereplői közötti adatmozgások

Az egyes szereplők közötti adatmozgásokhoz és a közöttük lezajló folyamatok leírásához az ábra mellett a https://wiki.aai.niif.hu/index.php/ShibMessages címen elérhető wiki oldal ad útmutatást.

3.1 Felhasználó → SP

A felhasználó lekéri a védett szolgáltatást, azonban a Shibboleth modul közbeavatkozik, mivel a felhasználó még nem azonosította magát és így nem rendelkezik a Shibboleth session-nel. A session állapotinformációt fejez ki a felhasználóról, megadva egy már megtörtént azonosítási folyamatot, illetve azt, hogy a felhasználó éppen melyik szolgáltatást veszi igénybe. Az SP beállít egy cookie-t a felhasználó gépén, ami alapján később rekonstruálható, hogy a felhasználó milyen szolgáltatást (URL) akart igénybe venni.

Mivel még nem lehet tudni a felhasználót azonosító IdP-t, ezért az SP átirányítja a felhasználót az Discovery Service-hez.

3.2 Felhasználó → DS

A Discovery Service felsorolja pl. egy legördülő listában a felhasználó részére a választható IdP-ket (a DS olvasható IP cím alapján előválasztást végez, valós időben megtippeli, hogy a felhasználó, milyen IdP-nél kívánja azonosítani magát), majd a megfelelő IdP kiválasztása után ezt egy cookie-ban eltárolja, amennyiben a felhasználó bejelölte, hogy a DS jegyezze meg a választást a munkamenet (session) végéig. (Lehetőség van arra is, hogy megmaradó cookie-ban tárolja a kiválasztott azonosító szervezetet (IdP-t).) A föderációban lehetőség van több DS használatára, lehetséges továbbá egy, ez előzőekben leírt előválasztó felület alkalmazása is.

Lehetőség van továbbá arra is, hogy egyes intézmények a saját maguk üzemeltessenek DS-t, továbbá arra is, hogy az intézményi DS mellett egy központi DS is működjön.

A választás eredményeként DS válaszol az SP-nek, az pedig SP átirányítja felhasználót az IdP-hez.

3.3 Felhasználó → IdP

Felhasználó megadja az azonosító nevét és a jelszavát és ez alapján kap egy sessiont.

3.4 Felhasználó → SP

Az IdP és az SP közötti üzenetváltások a felhasználó browser-én keresztül történik. A két entitás közötti kommunikáció vagy (i) artifact használatával, vagy (ii) HTTP POST alkalmazásával történik.

Az SP SAML autentikációs kérést, AuthN request-t küld az IdP-nek. Az AuthN request-ben szereplő ID-re (egy véletlen szám) érkezik válasz a SAML Response-ban. Ezek az AuthN requestID-k egyszer használatosak, le is járnak, amely lejáratra egy fix időpont van meghatározva. Az IdP oldalán a felhasználónak munkamenete jön létre, amelyre IdP implementációnként eltérő megoldás lehetséges.

Az IdP maga dönti el, hogy mi a kiadható attribútumok köre az adott SP felé - az attribútumok köre az AttributeReleasePolicy-ben (ARP vagy Filter) található (l. Azonosítók).

3.5 SP →IdP

Az SP SOAP kapcsolatot nyit az IdP ArtifactResolutionService URL-jére, ahol az Artifact alapján megkapja a teljes SAML response-t.

A SAML Response (attribute push), attribute push post profile esetén ajánlott a titkosítás.

3.5.1 Artifact

Az IdP artifact üzenetét ellenőrzi az SP, majd - amennyiben a felhasználó jogosult az erőforrás igénybevételére - az SP tovább irányítja az alkalmazáshoz. SP-IdP irány

mindenképpen titkosított (HTTPS), itt az assertion nem titkosított. Az IdP - Sp irányban az artifact nem titkosított. SP indít egy SOAP kérést az IdP felé, amivel az artifact-hoz tartozó assertion-t (és benne a felhazsnáló adatokat) elkéri. Létrejön egy SP oldali session, ehhez a böngészőben cookie tartozik (_shibsession_). Az artifact tulajdonképpen egy hivatkozás egy asssertion-re, amit az IdP HTTP GET-el küld az SP-nek, szintén felhasználó böngészőjén keresztül. Az SP artifact esetében, tehát a felhasználói attribútumok nem a felhasználó böngészőjén keresztül, hanem a közvetlenül az IdP-től jutnak el az SP-hez.

Az IdP a felhasználó böngészőjén keresztül küldi el az artifactot az SP-nek, az üzenetváltás során nem kötelező az artifact üzenet titkosítása (SSL használata nem kötelező), de az SP-től érkező SOAP hívás (ami már nem a felhasználón keresztül megy), egy kötelezően titkosított, kölcsönösen hitelesített csatornán keresztül történik. IdP válaszként az SP-nek assertiont küld vissza szintén titkosítva megy.

3.5.2 Http POST

Választhatóan titkosítva küldi az IdP az attribútumokat az SP-nek, azonban nem minden alkalmazás támogatja a titkosítást. Csak akkor tudja titkosítani az IdP az üzenetet, hogy ha a metadatok között be van ágyazva az SP teljes tanúsítványa. Ha HTTP POST-ot használ a két fél és ez a post titkosított helyre meg, akkor nem kötelező titkosítani az üzenetet, ha nem HTTPS portra megy az üzenet, akkor kötelező titkosítani az üzenetet. A titkosítás lehetővé teszi, hogy a böngésző hibái esetén is védettek maradnak a felhasználói adatok. Ezért HTTPS esetén is ajánlott, hogy titkosított POST-ot használjanak a szereplők.

A crypt használatát az IdP dönti el, a föderációs követelményekben benne lesz, hogy crypt nélkül nem küldhetnek HTTP POST-ban üzenetet illetve megoldás lehet a HTTP crypt betiltása. Utóbbira azért lehet szüksége, mert hogy ha crypt nélkül küldik el a HTTP POST üzenetet, akkor fennáll a veszélye annak, hogy személyes adatok kiszivárognak.

Probléma lehet, hogy ebben az esetben a cryptelést a föderáció csak előírni tudja, de kikényszeríteni nem.

3.5.3 Föderációs követelmények a végpontokkal kapcsolatban

1. IdP SSO URL (autentikáció) – HTTPS kötelező

2. IdP Attribute Authority assertion/attribute query – HTTPS kötelező

3. SP artifact resolution service – nem kötelező a HTTPS

4. SP assertion consumer service – HTTP + crypt-el (nem javasolt a megoldás a böngésző warning miatt) vagy HTTPS (crypt javasolt)

Az, hogy az SP melyik binding-ot képes használni az a metadata-ban van benne. Az autentikációs üzenetben (Auth Query benne van, hogy az SP konkrétan melyik végpontra kéri a válaszüzenetet).

4 Metadata

4.1 Metadata a Föderációban

Maga a föderáció lényege a metadata, ebben van leírva, hogy kik a résztvevők, SAML szabványnak mely részeit támogatják és hogy az IdP-k és SP-k milyen URL-en és binding-al szólíthatók meg. A metadata tartalmaz intézményi adatokat is, valamint az egyes intézmények technikai és adminisztratív kontaktjainak elérhetőségi adatait. A NIIF AAI metadata az alábbi címen érhető el: https://idp.niif.hu/href-idp-metadata.xml

A személyes adatok köre:

- név
- email cím

A metadata teljesen publikus, a föderáció által aláírt állomány. (Letöltéskor az IdP-knek és SP-knek ellenőrizniük kell az aláírást.) Felmerült, hogy a metadata-nak legyen fclhasználási feltételei.

Mindenki egy központi helyről rendszeres időközönként letölti a metadata fájlokat. A svájci SWITCH föderáció esetében pl. ha valamelyik entitás adminisztrátora nem tölti le frissített metadata-t, akkor figyelmeztetik.

A metadata-ban szereplő requested attributes információt az egyes IdP implementációk eltérően kezelik. (pl. simpleSAMLphp ez alapján genrálja a szűrési szabályokat, míg a Shibboleth IdP figyelmen kívül hagyja)

IdP-nél beállított Attributum Authority tartalmazhatja azon attribútumok felsorolását, amelyeket az IdP támogat. Az SP-knél tartalmazhat még a metadata, olyan paramétereket, amelyek megmondják, hogy az egyes SAML üzeneteket alá kell-e írni vagy sem.

A metadat-ban benn lehet a föderációban támogatott NameID formátum az azonosító általános értelmezése (tranziens, perzisztens, akár emailcím is lehet stb.).

A metadata-ban szerepel, hogy egy intézmány milyen scope-ot használhat. Vannak olyan attribútumok, amelyek scope-t is tartalmaznak és az attribútum értéke mellé oda van írva, hogy milyen tartományra érvényes.

Az SP ebben az esetben leellenőrzi, hogy a scope-ot valóban olyan IdP állította ki, amely jogosult az adott scope kiállítására (az ELTE nem állíthat ki bme.hu scope-os email címet), ennek azért van jelentősége, hogy az IdP működése is szabályozott keretek között történjen.

Fontos megjegyezni, hogy a föderáció maga dönti el, hogy hogyan állítja össze a metadatá-t.

A svájci SWITCH föderációban egy intézményi meghatalmazott (adminisztrátor) állíthatja össze az intézményi metadatá-t és ezekből áll össze a föderációs metadata. A svájci modell alapján egy központi adminisztrátor veszi fel az egyes IdP-ket a föderációba.

A metadata-nak nem válik részévé az ARP, viszont az ARP-t létre lehet hozni a metadata alapján. (Ez egy megengedő hozzáállás esetén jó megoldás. Ebben az esetben az IdP minden, a metadata-ban kért adatot odaad az SP-nek.)

A tervek között szerepel, hogy egy központilag üzemeltetett alkalmazás (Resource Registry), előre gyártott ARP-ket külön szolgáltatásként nyújtson az egyes SPknek. Emiatt fontos, hogy az SP-k előre megjelöljék egy központi felületen - Resource Registry - keresztül, hogy milyen attribútumra van szükségük. A Resource Registry alapján készül el a Föderáció által legyártott automatikus Filter (ARP) is. IdP adminisztrátora tehát választhat, kiadja az előre megadott attribútumokat azoknak az SP-knek, akiknek ezek az attribútumok kellenek. Amennyiben az IdP ki kívánja adni, az előre megadott attribútumokat az SP-nek, úgy egy előre kitöltött metadata fájl töltődik le. [Az SP megmondja mit akar, IdP dönt, de a központ gyártja le az ARP-t – a központban tárolt ARP-k távolról automatikusan frissíthető adatbázison keresztül érhetőek el. Az IdP adatbázisból kérdezi le, hogy van-e a számára új ARP.]

A föderáció alapelve, hogy mindenki autonóm módon dönthesse el, hogy milyen attribútumokat kér és milyen attribútumokat ad ki.

4.1.1 Attribútum specifikáció

A föderáció nagyon kevés adat esetében fogja megmondani, hogy kötelező egy attribútumot kiadni.

- állandó azonosító
- affiliation (intézményi státusz)
- intézmény típusa (kutatóintézet, egyetem stb.)

Az IdP egy már legenerált ARP alapján adja ki automatikusan az attribútumokat az SP-nek.

Az attribútumok köre az alábbi csoportokba sorolhatóak:

- kötelező attribútumok
- ajánlott attribútumok
- opcionális attribútumok

Attribútum specifikáció tervezte elérhető:

https://wiki.aai.niif.hu/index.php/HREFAttributeSpec

Belső eljárási rend kell arra vonatkozóan, hogy az újonnan csatlakozó SP által kért adatok egyáltalán kérhetők-e?

Ki a felelős az attribútumok valódiságáért? Attribútum specifikációban szerepelhetne az adat forrására utaló információ és az adat megbízhatósági szintjére vonatkozó utalás.

Autoritatív adatbázisból kell az IdP attribútum adatbázisának frissülni, hacsak nem az IdP attribútum adatbázisa az intézmény autoritatív adatbázisa.

Attribútum specifikációt össze kell vetni a a FIR (felsőoktatási információs rendszer) által tárolt adatokkal.

4.1.2 Metadata és a föderációk közötti együttműködés

Metadata egy központilag, automatikusan frissülő, aláírt struktúra; az aláíró kulcsot a föderációk megosztják a világgal. Jelenleg a föderációban több metadata forrást lehet megadni (mert a HREF-nél külön kezelik jelenleg az IdP-t, SP-t, TestIdP, TestSP, VHO), így az egyes szereplők megválaszthatják hogy kivel akarnak szóba állni (azt a metadata forrást le kell töltenie, amely alkalmassá teszi a két szereplő közötti kommunikációt). Az EduGain is egy ilyen opcióként fog valószínűleg megjelenni, ez pedig meghatározhatja, hogyan kapcsolódnak más föderációk a HREF-hez. Általában fenntartanak egy közös föderációs metadata halmazt, amelybe több föderáció metadatája található meg.

5 Azonosítók

Az azonosítókat az alábbi jellemzők alapján lehet csoportosítani:

1. transient – persistent
2. SP-ként azonos vagy különböző
3. SAML üzenet fejlécében megy vagy attribútumban.

A fenti csoportosítás alapján pedig a következő azonosítókat különböztethetjük meg:

5.1 Transient NameID

Csak IdP – SP közötti kapcsolatban használatos, a NameID alapján tud visszakérdezni az SP az IdP-től, pl. ha nincsen meg minden attribútum; ez alapján lehet visszakövetni a felhasználót; a NameID általában egy teljesen random string – az IdP a timestamp és a saját nyilvántartása alapján vissza tudja követni, tranziens, egyáltalán nem jellemző a személyre. IdP nélkül ilyen típusú azonosító esetén az SP az azonosítóból nem tudja megállapítani, hogy ki volt a felhasználó.

5.2 Azonosító jellegű attribútumok

Bármilyen információt használhat az SP azonosítóként. Pl. email cím; ezt használhatja az SP azonosítónak is, így az azonosító attribútumként kerül átadásra, minden SP ugyanazt kapja meg (non-targeted).

5.3 ePPN (EduPersonPrincipalName)

Lokális állandó azonosító, amely tartalmazza az IdP intézmény domain nevét, amely megegyezhet az email címmel, de nem feltétlenül. Több föderáció használja, azonban nem tűnik jó gyakorlatnak, mivel könnyen beazonosítható a felhasználó általa.

5.4 Föderációs egyedi azonosító (fooUniqueID)

A föderáció generálja le, nem jellemző a személyre, attribútum definíciója garantálja, hogy egyedi legyen – attribútumként kerül átadásra, minden SP ugyanazt kapja meg (non- targeted). A NIIF AAI föderáció nem kívánja ezt használni. (Egyébként létezik niifUniqueID, ezt csak lokális ldap-okban használják vagy egyes intézmények ezt használják a saját azonosítók helyett. A niifUniqueID-ból nem lesz föderációs egyedi azonosító.)

5.5 ePTID (EduPersonTargetID)

Ez pontosan ugyanaz mint a SAML persistent NameID, csak nem az assertion subject-jében, hanem attributumként átadva. Perzistens , átlátszatlan, targeted azonosító.

A SAML két verziója esetében eltérően kezelődik, ami okozhat kompatibilitási problémákat: régi: <AttributeValue scope=”SP” >1234</AttributeValue> új: <AttributeValue><**NameID>....</NameID>**<AttributeValue>

5.6 Persistent NameID

A PersistentNameID alkalmas állandó azonosítóként való használatra.

Cél, hogy minden SP-nek különböző azonosítót kell megkapnia (targeted) és ennek az azonosítónak átlátszatlan (opaque) kell lennie.

Az IdP eltárolja, hogy egy meghatározott felhasználóhoz kötődő azonosítót egy adott SP-nek már kiadott.

Az állandó azonosítók azért szükségesek, mert bizonyos alkalmazások (pl. wiki) számára specifikus attribútumok használata is szükséges lehet. Állandó azonosítók kötik össze a két adatbázist (IdP DB és SP alkalmazás DB) – felhasználóra nézve azonosnak kell lennie. Szükséges a két pont között kell egy kulcs, ami az állandó azonosító lehetne (ezt az azonosítót általában a felhasználó gépeli be – emiatt egy olvasható, megjeleníthető azonosítóként akarják kezelni az alkalmazások).

Fontos cél a HREF föderáció esetében, hogy ne legyen ez a kulcs olyan személyes azonosító, amely alapján a felhasználó könnyen beazonosítható. Használhatósági szempontként megjegyzendő, hogy az alkalmazások nem föderatív szerepre vannak felkészülve, targeted és az opaque azonosítók nem humán olvasására vannak tervezve.

Megjegyzendő, hogy az az adat, amelyet kiad az IdP az SP-nek és amely ugyan felhasználóra nem jellemző a magyar adatvédelmi szabályozás szempontjából mégis személyes adatnak minősül, továbbá mindaddig személyes adatnak minősül, amíg kapcsolata az érintettel helyreállítható.

Kérdésként merült fel, hogy ez a személyes adat, hogyan interpretálható a felhasználó felé humán által olvasható formában, technikailag nem kifejezetten lehetséges ez az átalakítás (privacy preserving ID – adatvédelembarát azonosítók). Itt jegyzendő meg, hogy nem ennek az adatnak kell humán által is olvasható formátumba megjelennie, hanem az adatkezelés folyamatát, az adat életútját kell tudni röviden és érthetően feltárni a felhasználó számára, hogy az így felvázolt adatkezeléshez egyértelműen hozzá tudjon járulni.

Általában, hogy ha az SP nem kapja meg az összes adatot, amire szüksége van, akkor közvetlenül kéri a szükséges adatokat a felhasználótól, ebben az esetben az állandó azonosító összeköthető a felhasználó által megadott adattal.

Kérdésként merült fel, hogy az SP által még elkért adatokhoz való hozzájárulás esetében, mihez járul hozzá a felhasználó, illetve, hogy ezzel kapcsolatban a Föderációnak milyen szinten kell a követelményeket megfogalmaznia (ajánlás vagy kötelező előírás). A kérdés alapján egy konkrét javaslat igénye fogalmazódott meg, így tehát, hogy mit tartalmazzon ez az előírás az IdP védelme érdekében.

Kérdésként fogalmazódott meg tovább, hogy elő kell-e írnia a föderációnak az IdP-k védelmében, hogy csak olyan SP-ket vesznek fel, akik a felhasználó hozzájárulását elkérik és az adatokat is kezelik, további kérdés, hogy itt milyen plusz kötelezettséget írhat elő a föderáció.

A fentiekkel összhangban, ajánlatos az EduPersonPrincipalName helyett vagy a SAML üzenet NameID-ját vagy az ePTID - EduPersonTargetedID használata.

Kompatibilitási igényként jelentkezik, az EduPersonPrincipalName használata, ha a NIIF egy másik föderációhoz akarna csatlakozni (interföderáció) – pl. északi szövetség, kalmár unió. Azonban igényként fogalmazódott meg, hogy a HREF az EduPersonPrincipalName-et csak az egyes intézményeken belül használják.

Az IdP-nél alkalmazott felhasználói user consent a uApprove, azonban a Shibboleth IdP mellett, a Simple SAML PHP ún. user consent modul-ja is használható.

Resource Registry[2] az ahol az SP megadja, hogy milyen attribútumokra van szüksége, így amikor az SP csatlakozik a Föderációhoz, megjelöli, hogy milyen - kötelező és opcionális felosztásban meghatározott - attribútumokra van szüksége. Elvileg lehetőség van arra, hogy a user consent modul átalakítására, hogy ezt az információt feldolgozzák és az opcionális attribútumokat a felhasználó le tudja tiltani, azonban ennek az implementáció nem egyszerű.

A megbeszélések során javaslatként fogalmazódott meg:

Minden szervezet a saját maga által megválasztott azonosítót használhatja, azonban a föderáció megfogalmazhatja valamilyen ajánlás formájában azt, hogy pl. a HREF az ePTID azonosítót preferálja, továbbá a föderáció nyilvántartást vezetünk arról, hogy az egyes SP-k milyen azonosítót használnak.

Problémaként vetődött fel a szabad azonosítóválasztással kapcsolatban, hogy az azonosító típusok alkalmazása közötti váltás technikailag nehezen kivitelezhető pl. átmeneti időszak, amikor két különböző azonosítót is használ az adott szervezet, ebben az esetben, fontos előfeltétel, hogy az SP kezében tartja az alkalmazást (ez pl. kereskedelmi szolgáltatás esetében nem lehetséges) Föderációhoz való SP szolgáltatás csatlakozás szükségessé teheti az azonosító típusok közötti váltást.

6 Központosított föderációk jellemzése

6.1 Központosított föderáció

Minden adatot a központba küldenek, amely rendelkezik egy olyan felülettel ahol a felhasználó hozzá tud járulni ahhoz, hogy az elküldendő adatokat elküldheti-e az Idp

[2] L. továbbá IAlkalmazási elemek funkció és II. Metadata

az SP-nek. Ebben a rendszerben minden IdP azonosít, de az összes adatot a központnak küldik el, így maga az IdO nem tárol adatot, csak irányít és továbbít, illetve a felhasználónak ad egy olyan felületet, ahol a hozzájárulásukat meg tudják adni. Központ azt tárolja, hogy egy bizonyos felhasználó, ez meghatározott SP esetében, egy meghatározott adatkör odaadásához hozzájárult-e már.

pl. Dán (wayf.dk) – tendencia a központosított föderáció, ez igényli a legkevesebb munkát az intézményektől.

6.2 Nem központosított (laza) föderáció

A laza föderációk esetében nincsen központi szervezet, amely az előzőhöz hasonló feladatokat látna el, és látszólag működés előfeltétele egy az előző szervezeti struktúránál nagyobb költségvetés is. pl. UK, USA, SWITCH , AUS.

7 Felhasználói hozzájárulás

I. UseCase:

Megszűnt a diák hallgatói jogviszonya, de szeretné az SP-vel továbbra is fenntartani a kapcsolatot, hogyan tudja azonosítani magát a felhasználó a jövőben NEM az IdP-n keresztül?

Megoldás:

1.Account linking. Elméleti megoldás van, azonban a gyakorlatban nem használható. (Valami miatt legalábbis ezt nem használják.)

2. Drupal tartalomkezelő rendszer integrálása a Shibboletthez. A felhasználó közvetlenül bejelentkezhet a Drupal-ba és ezt követően rendeli össze az aktuális session-t az IdP azonosítóval.

Jelenlegi gyakorlat az, hogy a felhasználónak van az SP-nél profilja és amint az SP csatlakozik a föderációhoz, onnan a felhasználó már nem közvetlenül az SP-hez megy, hanem az IdP–n keresztül; ebben az esetben az SP az IdP által generált humán által nem olvasható azonosítót összeköti az SP-nél már meglévő profillal (helyi azonosítóval) (mapping útján) – ha ez sikerült, akkor ennek a folyamatnak visszafelé is működnie kell.

MOST csak alkalmazás szinten megvalósítható a Drupal mapping, tehát csak alkalmazás felkészítésével lehet ezt az összekapcsolást megoldani.

II. Usecase:

További kérdésként merült fel az attribútumok aggregálásának igénye is, vagyis, hogy egy felhasználóról az SP több IdP-től is kaphasson adatokat (adat-összekapcsolás).

MIRE használj az SP az azonosítón kívüli attribútumokat:

- autorizáció
- tárolja és maga jeleníti meg ezeket az adatokat (pl. regisztrációnál)
- az SP által bekért adatok

- IdP hozzájárulást kér, hogy kiadhassa az adatot
- SP hozzájárulást kér, hogy tárolhassa az adatot

IdP előállítja a válaszüzenetet, aláírja és mikor már éppen elküldené, akkor közbeékelődik a modul, egy már előállított üzenet elküldéséhez tud a felhasználó hozzájárulni vagy a hozzájárulását megtagadni. Ebben a kialakított rendszerben változtatni nem lehet könnyen, technikailag nehéz közbeékelni egy felhasználói hozzájárulást kérő alkalmazást, a már elkészült üzenethez.

Az attribútumok kiadása az alábbi folyamat szerint zajlik le:

- Az DB-be (adatbázis) beleírja az intézmény az adatokat vagy beleírja a felhasználó
- Attribute Resolver tartalmaz minden attribútumot a felhasználóról
– Filter [Attribute Release Policy] (megkapja az attributumokat és tudja, hogy ki az SP) alapesetben a Filter mindent kiszűr; [vannak olyan központosított föderációk, ahol a Filter-t egy központosított rendszer, maga a Föderáció állítja elő] az IdP-től csak az SP specifikus attribútumok mennek ki az SP-hez
- Ezt követően jöhet közbe a uApprove (userconsent) - ha bejön egy új attribútum, vagy megváltozik a Terms of Use, akkor feljön ez a uApprove

Ha van uApprove, akkor az adatok bekérése idején, nem szükséges hozzájárulást kérni a felhasználótól. A uApprove-on belül, ahhoz is hozzájárulhat a felhasználó, hogy az IdP-nél a uApprove-al elfogadott adatokat helyileg is tárolják.

Ha nincs uApprove, akkor a DB felvételekor tájékoztatóra van szükség és azt kell mondani, hogy az SP szolgáltatásának igénybevételével hozzájárul, az adatok

elküldéséhez (tehát ahhoz, hogy az IdP elküldi az SP-nek). A tájékoztató a célhoz kötöttség mellett leírja azt is, hogy mi fog történni az adattal, az adatkezelés időtartamának meghatározásával együtt.

8 Felsőoktatási intézményen belüli adatkezelés

Kérdésként merült fel:

- Az intézményen belüli felhasználásnál kell-e hozzájárulást kérnie az intézménynek.

- Származtatott azonosítókat meg kell-e jeleníteni (human által olvasható formában) ezen a uApprove felületen.

A felsőoktatásról szóló 2005. évi CXXXIX. törvény 34.§-a tartalmazza a felsőoktatási intézményekben történő adatkezelés alapvető szabályait, valamint a felsőoktatás információs rendszerre vonatkozó előírásokat.

A hivatkozott rendelkezés alapján a felsőoktatási „**intézmény kezelheti a hallgató személyének azonosítására és elérhetőségére szolgáló adatokat (név, születési hely, idő, állampolgárság, állandó lakóhely és tartózkodási hely, telefonszám), valamint a hallgatói jogviszonnyal összefüggő adatokat. Ez utóbbi körben <u>különösen</u> a felvételeivel kapcsolatos adatokat, hallgató tanulmányainak értékelését és minősítését, a vizsgaadatokat, a hallgatói fegyelmi és kártérítési ügyekkel kapcsolatos adatokat.”** Más törvények az intézmény számára kötelezően előírják bizonyos személyes adatok kezelését, bizonyos esetekben köteles például nyilvántartani a hallgató adóazonosító jelét, társadalombiztosítási azonosító számát, mivel bevallási, illetve a különböző fizetési kötelezettségének csak így tud eleget tenni.

Minden más adatot csak akkor kezelhet az intézmény, ha ahhoz az érintett előzetesen hozzájárult. A kezelt adatokat csak akkor lehet az intézményen kívülre továbbítani, ha az érintett ehhez előzetesen hozzájárult, illetve ha az adattovábbítást törvény előírja.

A föderáció működésével kapcsolatban megvizsgálandó a felsőoktatási törvény felhatalmazása alapján a felsőoktatási intézmények részére engedélyezett adatkezelés, illetve a kezelt adatok köre, valamint a föderatív együttműködés során a személyes adatok kezelésének kapcsolata.

Különösen fontos e körben kitérni arra, hogy egy föderatív szolgáltatás igénybevétele során történő adatkezelés mennyiben tekinthető a hallgatói jogviszonyon alapuló, törvényi felhatalmazás alapján történő adatkezelésnek.

„Oscar” szolgáltatás csak SP-ként működik és van helyi adatbázisa, ami a szolgáltatáshoz tartozik, ebben nincsenek azonosítók, alkalmazás specifikus adatbázis (ezért nem IdP), hasonló még pl. a tudományos folyóirattár (ők csak az egyetemeknek szolgáltatnak szolgáltatást, felhasználóknak nem). Azok az SP-k ahol szükség van perzisztens azonosítóra, saját maguk, helyileg is tárolják azokat.

Javaslat: A SP nem csak azt adja meg, hogy milyen adatokat szeretne, hanem azt is meg kellene mondania, hogy mi célból kéri ezeket az adatokat (nyilvános információ) – és ezt a plusz információt is meg kellene jeleníteni (pl. comment) a uApprove-ban vagy/és a uApprove ad egy linket az SP adatkezelési szabályzatához.