Autentikációs és autorizációs infrastruktúrák

BAJNOK KRISTÓF

MTA Sztaki, ITAK
kristof.bajnok@sztaki.hu

Kulcsszavak: autentikáció, autorizáció, identitás menedzsment, föderáció, biztonság

Egy intézmény alapvető érdeke, hogy az általa nyújtott szolgáltatásokhoz, illetve bizalmas információkhoz csak megfelelő azonosítás után férhessenek hozzá a felhasználók. Heterogén felhasználási környezetben hatékony azonosítást és jogosultság-ellenőrzést úgy lehet megvalósítani, ha erre önálló infrastruktúrát, middleware-t alkalmazunk. A cikk bemutatja ennek fontosságát és vázol néhány, más országokban már általánosan elterjedt identitás szövetségi (föderációs) modellt.

1. Bevezetés

Az informatikai rendszerek terjedésével és jelentőségük növekedésével együtt a felhasználók azonosítása és jogosultságaik megfelelő ellenőrzése alapvetően fontossá vált. Az informatikai biztonsággal kapcsolatos számtalan kutatásból azonban megállapíthatjuk, hogy sok esetben a biztonság legnagyobb veszélyeztetője maga a felhasználó. Lehet ugyan a mai tudományos vélekedés szerint többé-kevésbé védett rendszereket készíteni, de a biztonság sok esetben rugalmatlanságot, nehéz kezelhetőséget jelent, ami rendkívüli módon növelheti a költségeket; másfelől a felhasználó munkájának nehezítése bonyolult azonosítási eljárásokkal végső sorban éppen magát a megcélzott biztonságot áshatja alá. Ezért óriási nyomás nehezedik az iparra és a kutatókra, hogy olyan azonosítási megoldásokkal álljanak elő, amelyek egyszerre képesek megvalósítani a következő – olykor egymásnak ellentmondó – követelmények optimálishoz közeli kompromisszumát: *kriptográfiai megbízhatóság; a felhasználó számára egyszerű használat; rugalmasság, könnyű karbantarthatóság; szabványosság, kompatibilitás; költséghatékonyság.*

A cikk bevezető jelleggel – és a téma szerteágazósága miatt messze nem teljeskörűen – ismerteti az autentikációs és autorizációs infrastruktúrákban (AAI) gyakrabban használt eljárásokat, valamint vázolja az intézmények közötti megállapodások (föderációk) elterjedtebb modelljeit.

2. Autentikációs middleware

Kezdetben az alkalmazásokat saját azonosítási funkcióval szállították, azonban ez súlyos problémákat vetett fel. Egyrészt a megfelelő erősségű hitelesítési eljárást implementálni kellett (minden egyes alkalmazásban), másrészt számtalan felhasználói adatbázis jött létre, melyek konzisztenciáját nagyon nehéz volt biztosítani. Ez utóbbi problémát leginkább úgy lehetett kiküszöbölni, hogy a felhasználói információkat valamilyen központi adatbázisban (NIS, SQL, illetve címtárak) tárolták. A címtárakat először az ITU X.500 szabványa írta le (amely lekérdezéshez a DAP – Directory Access Protocolt definiálta), elterjedt és könnyen hozzáférhető implementációja azonban csak az LDAP-nak (Lightweight Directory Access Protocol [1]) készült el. A címtár lekérdezések szabványosításának jelentős előnye a hagyományos adatbázisokhoz képest éppen maga a *szabványosság*, azaz,, hogy a kliens bármelyik gyártó szerverétől (elvileg) pontosan ugyanúgy tud adatokat lekérdezni.

A központi felhasználó-adatbázisokban (vagy azokhoz kapcsolódóan) nem csak az azonosításához szükséges adatok tárolhatók, hanem – több más adat mellett – a felhasználó jogosultságai is, akár alkalmazásonként külön-külön. Ha az adatbázis elé megfelelő felhasználói felületet készítünk, akkor megoldható, hogy a felhasználók hozzáadása/törlése, illetve jogosultságainak beállítása ne a rendszergazda feladata legyen, hanem részévé váljon az intézmény humánerőforrás-kezelési és belső házirend (policy) kezelési folyamatainak. Ha az intézmény alkalmazásai központi felhasználó-adatbázist használnak, és ezt az adatbázist a humánerőforrás és a házirend nyilvántartásáért felelős adminisztrátorok tartják karban, akkor *identitás-menedzsmentről (Identity Management)* beszélhetünk.

Az intézményi identitás-menedzsment bevezetése alapvetően fontos az informatikai biztonság szempontjából is. Ugyan nagyon kellemetlen (és pazarló), ha egy új munkatárs azért nem tudja megkezdeni a munkát, mert még nem kapott jogosultságot a megfelelő alkalmazásokhoz, ennél sokkal nagyobb károkat tud okozni egy elbocsátott dolgozó, akinek nem szűnik meg azonnal a hozzáférése az üzletileg kritikus rendszerekhez.

3. Webes Single Sign-On

Egyre több helyen használnak belső vállalati környezetben webes alkalmazásokat. Azonban hiába van központi felhasználói adatbázis, az azonosítást min-

den egyes alkalmazásnál külön-külön el kell végezni. Sok esetben ez a felhasználótól újabb és újabb közreműködést kíván. (A felhasználó szempontjából a több faktoros azonosítás még további gondot okozhat, ha az azonosítási módszer PIN-kód, esetleg idő alapú token megadását követeli meg – de még az ujjlenyomatolvasó túl gyakori használata is kényelmetlenné válik előbb-utóbb.) E problémákat általában úgy lehet megoldani, ha az azonosítást különválasztjuk az alkalmazástól, tehát az azonosítást nem az alkalmazásban végezzük el, hanem egy dedikált azonosító (login) szerveren.

A webes alkalmazásokhoz kidolgozott Single Sign-On (WebSSO) megoldások működésének alapjául a HTTP protokoll szabványos elemei szolgálnak: az átirányítás (redirect) és a sütik (cookie). Számos WebSSO szoftver létezik, például Pubcookie, CAS, A-Select stb. Az azonosítás menetét szemlélteti az *1. ábra*.

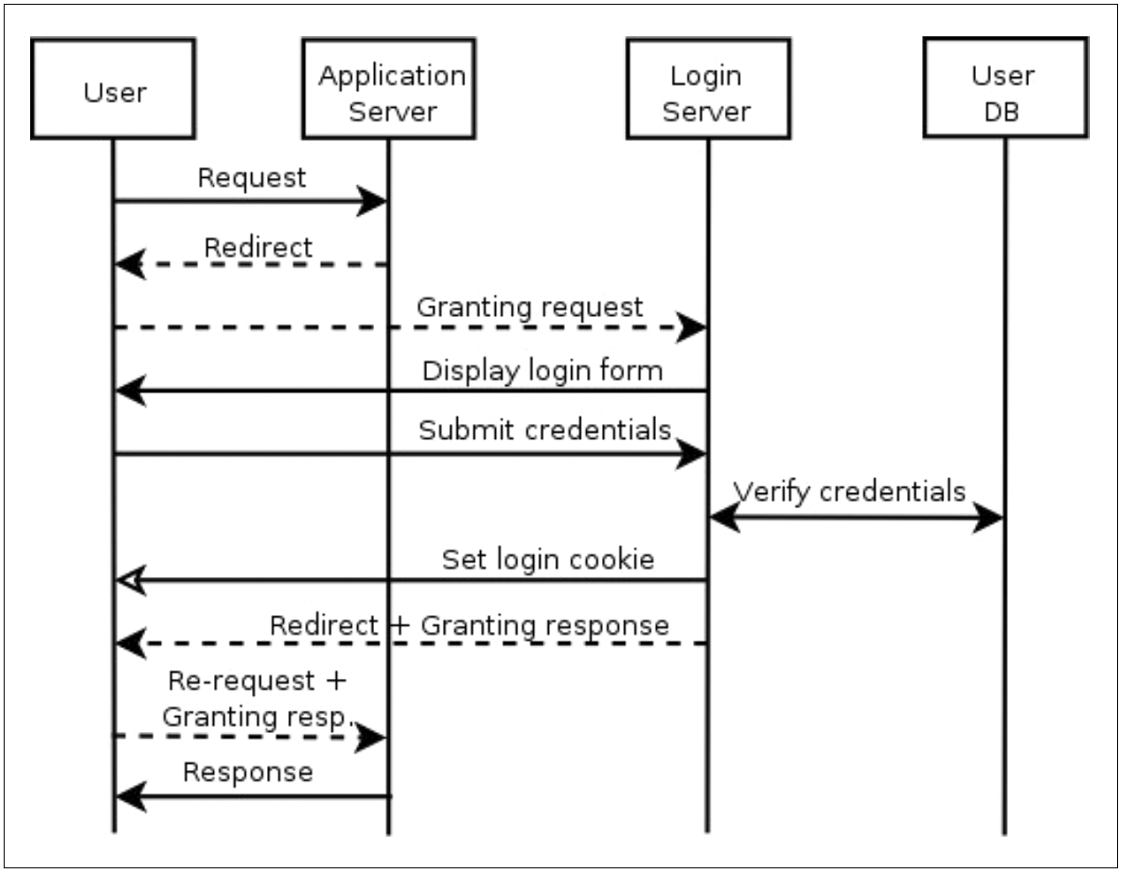
A felhasználó az azonosító adatait mindig a megbízhatónak tekintett login szervernek adja meg. Iső lépésként a webes alkalmazás előtt álló webszerver modul észleli, hogy még a felhasználónak nincs érvényes környezete (security context), ezért átirányítja a login szerverhez. Ez elvégzi az azonosítást, majd sikeres esetben készít egy úgynevezett feljogosító (granting) üzenetet az alkalmazás számára, majd ezt eljuttatja a webszerver modulnak. (Természetesen gondoskodni kell arról, hogy a granting üzenet ne legyen visszajátszható, ezért a válasz tartalmazza a requestben található véletlen elemet is.) A webszerver ezt ellenőrizve engedélyezi a hozzáférést az alkalmazáshoz.

Fontos megjegyezni, hogy ez a módszer csak a felhasználó azonosítást (autentikációt) oldja meg, a jogosultság kezelés (autorizáció) továbbra is az alkalmazás feladata marad. A magát már azonosított felhasználó „beazonosítása” (azaz az autorizációhoz, illetve az alkalmazás használatához szükséges további adatok lekérdezése) a granting üzenetből kinyerhető azonosító alapján történik. (Hasonlóan működnek a HTTP Basic autentikációt használó webes alkalmazások is: ott a webszerver az azonosítás után a felhasználónevet a REMOTE_USER változóban adja át.) Ez azt is jelenti, hogy az alkalmazásnak a felhasználó attribútumaiért közvetlenül a felhasználó-adatbázishoz kell fordulnia.

Amennyiben a felhasználó másik alkalmazáshoz fordul, az ugyanúgy a login szerverre irányítja át, ám ezúttal a login szerver (a korábban beállított süti alapján) észleli azt, hogy a felhasználó már azonosította magát, ezért az azonosító adatok elkérése nélkül kiállítja a granting választ. Így a második autentikációhoz már nincs szükség a felhasználó közreműködésére.

Mivel a legtöbb WebSSO megoldás (memóriában tárolt) sütiket használ, ezért az alkalmazásból történő kijelentkezés megvalósítása korántsem egyszerű. Vannak szoftverek, amelyek lehetővé teszik az alkalmazásonként történő kijelentkezést, azonban számos esetben csak a böngészőből való kilépéssel (vagy a sütik törlésével) lehet kijelentkezni.

A WebSSO – noha tényleg egyszerűsíti a felhasználó számára az autentikációt – biztonságossága leginkább a böngészőben tárolt cookie-k biztonságán múlik. Fontos észrevenni, hogy a login szervernél érvé-



1. ábra

Webes SSO alkalmazás (PubCookie) működésének folyamata [2]

nyes munkamenetünket tároló süti nem védhető visszajátszás ellen, ezért annak lehallgathatatlanságáról gondoskodni kell. Sajnos a böngészőket érintő hibák egy része kihasználható a cookie-k ellopására is, azonban ezek a hibák – WebSSO-tól függetlenül – minden olyan alkalmazást érintenek, amelyeket webböngészőn keresztül veszünk igénybe (hiszen így tetszőleges sessiont el lehet lopni).

A WebSSO megoldások előnye, hogy nagyon olcsón, minimális költséggel kialakíthatók úgy, hogy a legtöbb alkalmazáson csak kismértékben kell változtatni. (A webszerver autentikációs moduljait használni képes alkalmazások például változtatás nélkül működhetnek.)

Az azonosítás biztonsága növelhető azáltal, ha a login szerver valamilyen erős autentikációs mechanizmust (például hardver tokenes megoldást) alkalmaz. Mivel ekkor a mechanizmust csak a login szerver számára kell implementálni, ezért a WebSSO megkönnyítheti az erősebb autentikáció bevezetését az intézményen belül, illetve jelentősen csökkentheti a bevezetés költségeit.

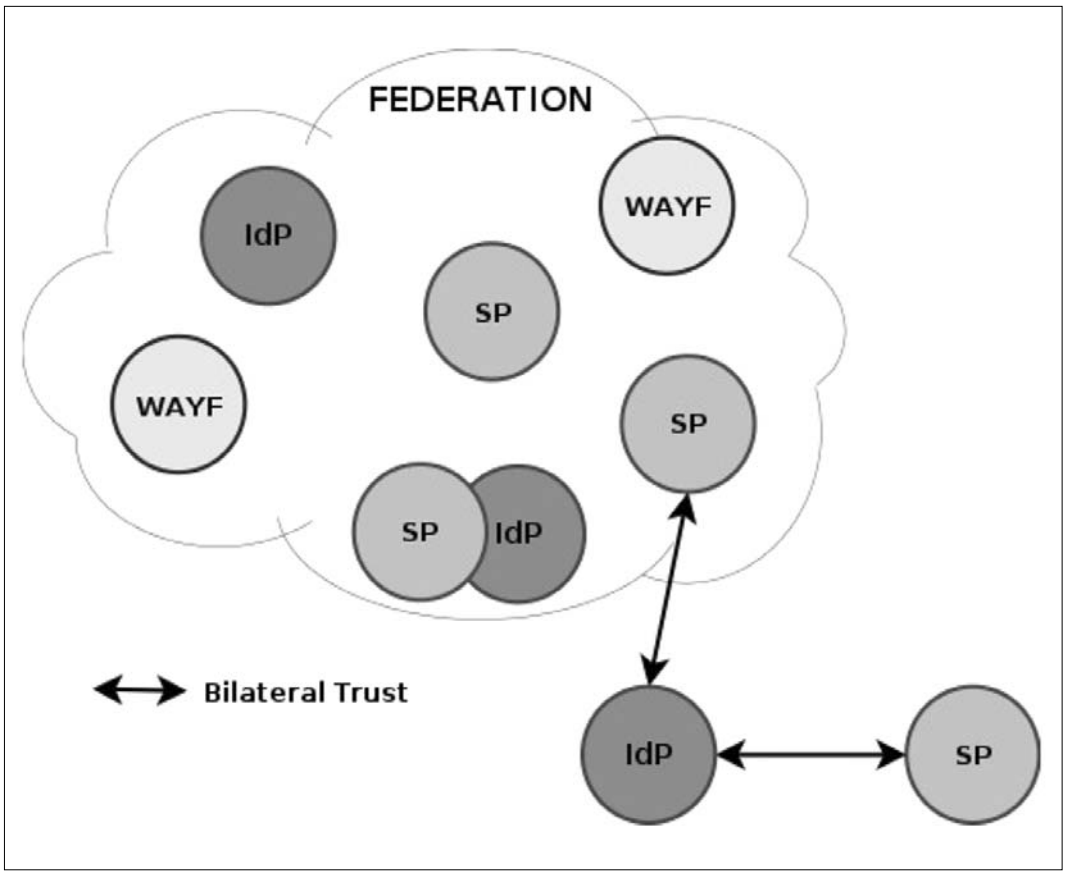
4. Föderációk

A cikk elején szót ejtettünk arról, hogy egy intézmény informatikai biztonságának alapja a megfelelő identitás-menedzsment. Gyakran előfordul azonban, hogy egy projekt megvalósításában több intézmény dolgozik együtt, és a munka során közösen használnak erőforrásokat. Más intézmények dolgozóinak saját adatbázisunkba való felvétele viszont számos problémát és nehézséget okozhat, hiszen például az egyik intézmény nem biztos, hogy értesíti a másikat arról, ha elbocsát egy, a közös projekten dolgozó munkatársat. Szintén a „befogadó” intézményt terheli a felhasználói panaszok kezelése (jelszóváltoztatás, bejelentkezési problémák), ezen kívül a felhasználónak új azonosító adatokat (felhasználónév/jelszó, chipkártya stb.) kell használnia.

A megoldást az jelentheti, ha a két intézmény szövetségre (Federation) lép egymással, és kölcsönösen *megbíznak* egymás identitás-menedzsmentjében. Nagyon fontos megérteni, hogy ez a „bizalom” nem elsősorban informatikai megoldásokon, hanem jogi kötelezettségvállalásokon alapszik. A megállapodás során a felek számtalan dolgot rögzíthetnek: az identitás-menedzsmentben használt eljárásokat, az alkalmazható autentikációs metódusokat, a felhasználóról kiadott attribútumok alkalmazásának feltételeit vagy akár rendelkezésreállási paramétereket. Természetesen a szövetségkötés nem csak kétoldalú lehet, hanem kettőnél több intézmény is együttműködhet.

Mielőtt a föderációk részletesebb ismertetését tárgyalnánk, érdemes észrevenni, hogy a „nem-digitális” világban is több helyen használnak bizalomra épülő föderációkat. Amennyiben A ország megbízik B ország „identitás-menedzsmentjében”, akkor B ország polgárai a B ország által kiállított azonosító okmányukkal (útlevelükkel) utazhatnak A-ba.

Természetesen előfordulhat, hogy két ország nem bízik meg egymásban: ekkor vízumot kell használni, a vízumot ugyanis mindig a fogadó állam (nagykövetsé-



2. ábra

Föderációs topológia. A nyilak kétoldalú (föderáción kívüli) bizalmat jelentenek

ge) állítja ki. A különbség világos: a vízum kiállítás körülményes és drága, ellenben nem szükséges hozzá bizalomra épülő kapcsolat.

Egy föderációban levő szolgáltatásokat funkciójuk szerint általában három osztályba sorolhatjuk. Vannak az *Identitás Szolgáltatók (IdP, Identity Provider)*, amelyek a felhasználó azonosítását végzik, illetve esetlegesen adatokat közölnek a felhasználóról a *Tartalomszolgáltatók (SP, Service Provider)* számára, amelyek közvetlenül a felhasználó számára nyújtanak (azonosítást igénylő) szolgáltatást.

Egy intézmény általában működhet egyszerre IdP-ként és SP-ként is. E két szolgáltatáson kívül lehetnek még olyan alkalmazások, amelyek a Föderáció működtetését segítik elő. Amennyiben egy Föderációban több egyenértékű IdP vesz részt, szükség van olyan alkalmazásra, melynek segítségével a felhasználó Identitás Szolgáltatója kiválasztható. Ez történhet implicit módon (például a felhasználónév hordoz információt az IdP-ről), illetve lehetséges olyan speciális alkalmazás használata is, amely első látogatáskor megjeleníti a felhasználó számára az elérhető Identitás Szolgáltatókat. Ezt a szolgáltatást *Home Location* szolgáltatásnak nevezzük, de elterjedt a „Where Are You From?" (WAYF) elnevezés is.

A Föderációban résztvevő elemek kommunikációjához általában szükség van *metaadatokra*, amelyek többek között tartalmazzák a szerverek közötti biztonságos adatkapcsolathoz szükséges PKI tanúsítványokat is.

4.1. SAML

Mivel egy Föderációban résztvevő intézmények általában szabadon dönthetnek arról, hogy milyen szoftvermegoldást alkalmaznak, szükség van arra, hogy az egyes elemek közti kommunikáció szabványos módon történjen.

2001-ben az informatikai ipar legnagyobbjai (Hewlett-Packard, Sun, Intel, Novell, Entrust, RSA stb) elkezdték kidolgozni a biztonsági kommunikáció nyílt szabványát, amelyet 2002-ben az OASIS szabványosítási szervezet *SAML (Security Assertions Markup Language* [3]) néven elfogadott. A szabvány jelenlegi, 2.0-ás verzióját 2005 márciusában fogadták el, ez jelentős újításokat hozott a korábbi, már működő rendszerekben használt 1.1-es verzióhoz képest. Funkcionális újítások mellett az új verzió leginkább azért érdekes, mert jelentős lépéseket tesz annak érdekében, hogy képes legyen integrálni meglévő megoldásokat (pl. Shibboleth, Liberty, ill. nagy gyártók Identity Management termékei) és szabványokat (WS-Security), így várható, hogy az AAI elemek kommunikációjának egyfajta „lingua franca"-ja lesz. Ez okból is érdemes a szabvánnyal részletesebben foglalkozni.

A SAML XML alapú keretrendszert definiál, amely autentikációs és jogosultsági adatok, valamint attribútumok szabványos kommunikációját teszi lehetővé. A keretrendszer tartalmazza az egyes elemek XML sémáját, valamint protokollokat és profilokat ír le. Mivel a SAML XML alapú, ezért így számos átviteli módszerhez illeszthető (binding).

Egy SAML üzenet legkisebb egysége az entitásra vonatkozó *állítás (statement)*, amely vonatkozhat autentikációra (Authentication Statement), a felhasználó valamely attribútumára (Attribute Statement), illetve valamilyen autorizációs döntésre (Authorization Decision Statement). Az állítás hordozhat paramétereket is, így például leírható, hogy az autentikált entitás milyen módszerrel lett azonosítva.

Egy SAML *igazolás (Assertion)* egy vagy több állítást tartalmazhat, kiegészítve a hitelesség ellenőrzését lehetővé tevő paraméterekkel: azonosító, kiállító (Issuer), kiállítás dátuma, „célközönség" (audience) stb. (Magyarítási megjegyzés: az angol „assertion" szó szinonímája a „certificate"-nek, amit a szakirodalom bevett módon tanúsítványnak fordít. Mivel tanúsítvány alatt általában X.509 tanúsítványt értünk, a félreértések elkerülése végett a cikkben az „assertion"-re magyarul az „igazolás" szót használjuk.)

Föderált környezetben az entitás megnevezése komoly problémákat vethet fel. Adatvédelmi okok miatt sok esetben tilos (és biztonsági megfontolások alapján sem célszerű) az entitásnak az IdP rendszerében érvényes azonosítóját átadni az SP számára, így legtöbbször egy felhasználói munkamenetre érvényes ideiglenes azonosítót (transient opaque identifier) alkalmaznak.

Az igazolás a hitelesítés érdekében opcionálisan tartalmazhat digitális aláírást is. A digitális aláírásra a szabvány a W3C XML Signature szabványának használatát írja elő. (Pontosabban az ebben definiált „enveloped signature" aláírási eljárást.) Felmerülhet a kérdés, hogy miért nem kötelező a digitális aláírás használata? A válasz az, hogy számos esetben már hitelesített a kommunikációs csatorna – például kölcsönös SSL hitelesítéssel –, így szükségtelen az egyes igazolásokat külön-külön aláírni.

SAML üzeneteket többféle módon továbbíthatunk az elemek között, a szabvány részletesen foglalkozik az egyes hordozó protokollokkal (bindings). Az alapvető üzenettovábbítási mód a SOAP (Simple Object Access Protocol), melyet leggyakrabban HTTP felett használnak. A szintén gyakran használt HTTP POST csatolásnak akkor van jelentősége, amikor a felhasználót – például az azonosítási eljárás során – át kell irányítani egyik kiszolgálóról a másikhoz. A csatolás lényege, hogy a webszerver olyan weboldalt állít elő, amely egy HTML form-ot tartalmaz, amelyet a felhasználó böngészője egy apró JavaScript kód segítségével automatikusan elküld a fogadó kiszolgálóra. A HTML form része egy rejtett változó, amely a tényleges SAML üzenetet tartalmazza.

A HTTP POST csatolás nagyvonalúan bánik a felhasználó sávszélességével, hiszen ekkor a teljes SAML üzenetet le kell tölteni a forrástól, majd azt el kell küldeni a célállomásnak. Ennek kiküszöbölésének érdekében definiálja a SAML az *Artifact* fogalmát, amely valójában egy hivatkozást, referenciát jelent az eredeti

SAML üzenetre. Artifact binding használatakor a felhasználó böngészője csak a (sokkal kisebb méretű) referenciát adja át a célállomásnak, majd az Artifact Resolution Protocol segítségével közvetlenül (általában SOAP segítségével) kérdezi le az eredeti SAML üzenetet.

5. Föderációs modellek

Alapvetően kétféle föderatív modellt különböztethetünk meg. *Központosított föderációnak* nevezzük azt a modellt, amelyben csak egyetlen identitás-szolgáltató található, minden más intézmény tartalomszolgáltató. Ilyen például a Microsoft Passport és a magyar elektronikus közigazgatás azonosítási rendszere, az Ügyfélkapu.

Mivel a központosított modellekben minden identitással az egyetlen IdP rendelkezik, annak megbízhatósága és helyes működése a teljes rendszer biztonsága szempontjából kritikus. Központosított föderációk esetén az egyes tartalomszolgáltatók nincsenek egymással összakapcsolva, köztük adatcsere nem történik.

Elosztott föderációról beszélhetünk akkor, ha egy föderáción belül több identitás-szolgáltató is működik. Ilyenkor az IdP-k jellemzően egyenértékűek, a hozzáférés szabályozása (autorizáció) az SP-knél történik.

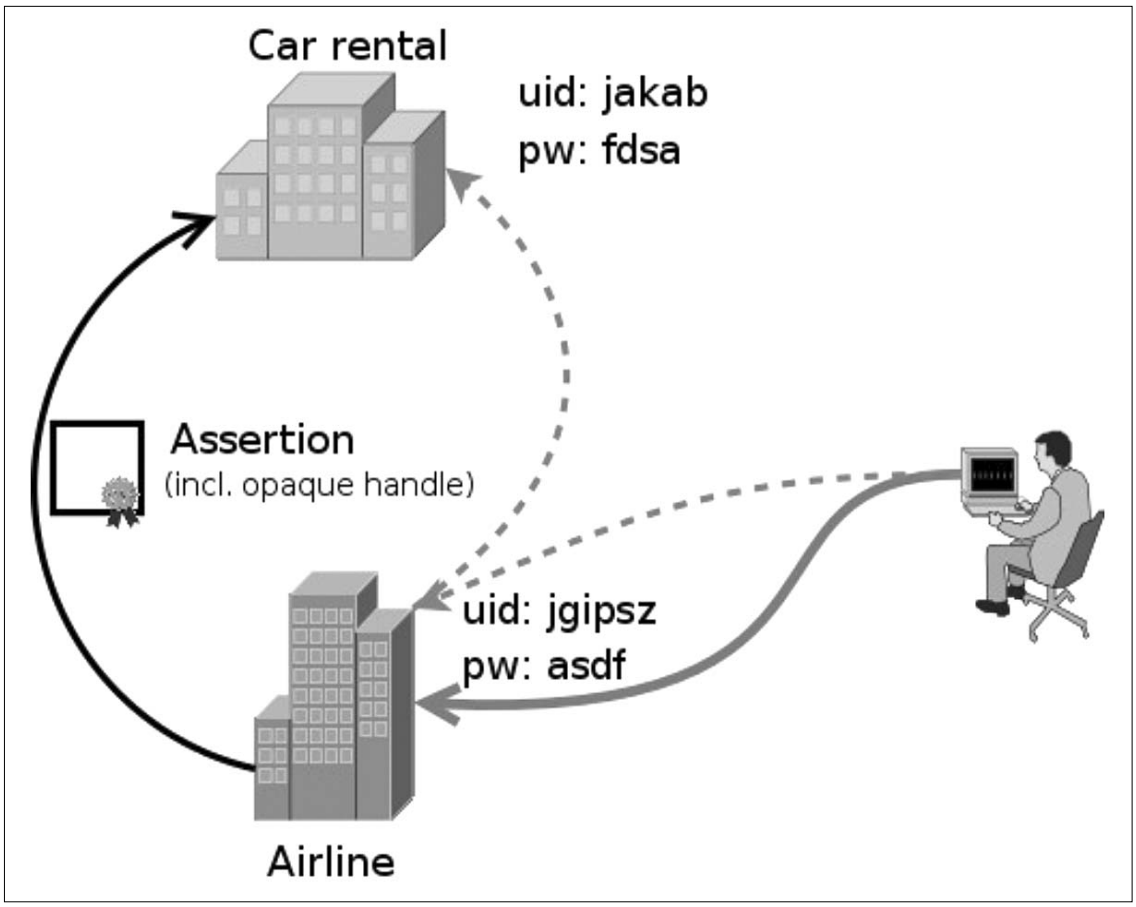
5.1. Liberty Alliance

A Liberty Alliance [4] projekt 2001-ben indult, korábban nem létezett nyílt szabványokra épülő identitás menedzsment federációs megoldás. Létrehozói elsősorban ipari cégek: Sun Microsystems, Hewlett-Packard, IBM, Intel, Oracle stb. A modell szerint a felhasználó különböző fiókokkal (account) rendelkezik különböző tartalomszolgáltatóknál, így mindegyik tartalomszolgáltató képes őt azonosítani, azonban az azonosító adatok szolgáltatónként különbözők lehetnek. A Liberty lehetőséget ad arra, hogy a felhasználó a különböző azonosítóit *összekapcsolja*, majd az SP-k szolgálatatásait egyetlen szolgáltatónál történő azonosítás után vehesse igénybe, tehát SSO-t biztosít. Lényeges megjegyezni, hogy ez az összekapcsolás kizárólag a felhasználó közreműködésével jöhet létre. Autorizáció kizárólag az egyes szolgáltatóknál található adatok alapján történik, adatcsere a szolgáltatók között csak annyi lehetséges, amennyi az összekapcsoláshoz, illetve az elosztott autentikációhoz szükséges.

5.2. Shibboleth

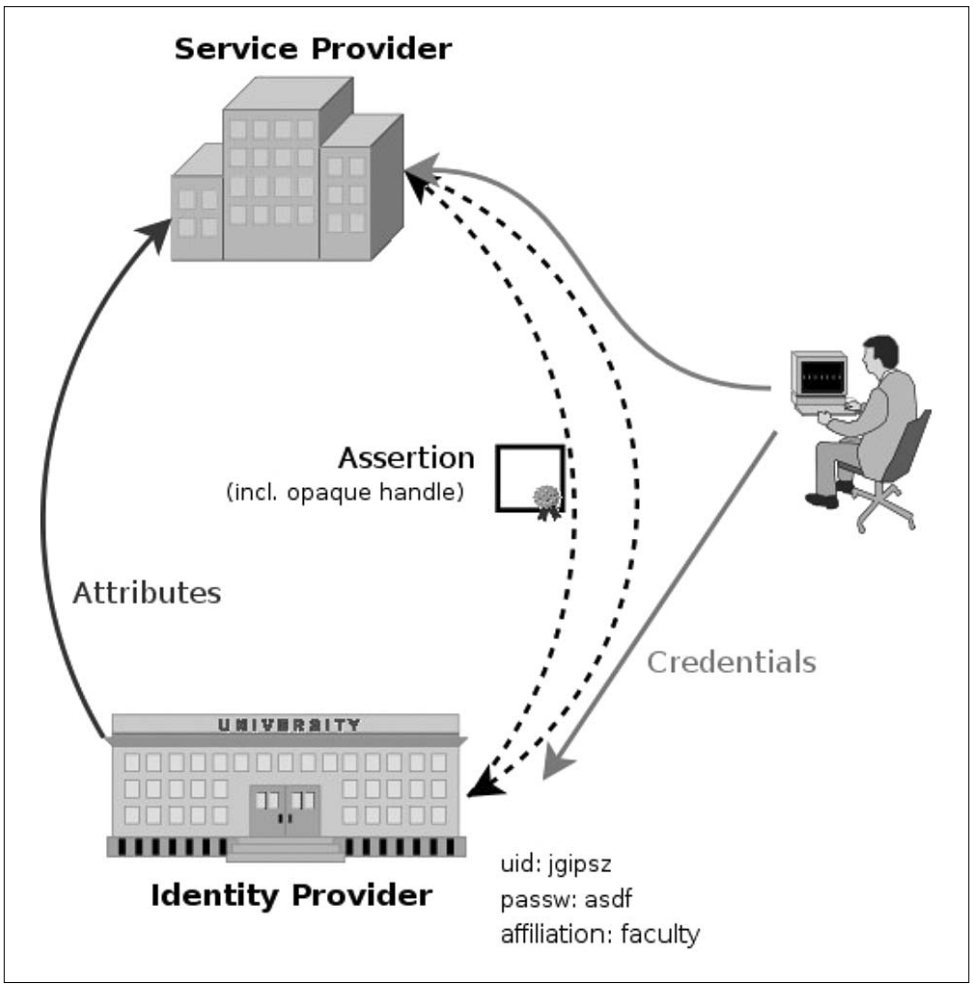
A Shibboleth projektet [5] az amerikai Internet2 indította. A Shibboleth egy elosztott autentikációs és autorizációs rendszer, ahol az erőforrásokhoz történő hozzáférés az identitás-szolgáltatótól kapott attribútumok alapján történik. A felhasználó úgy vehet igénybe szolgáltatásokat a föderáción belül, hogy csak egyetlen identitása van az „anyaintézménynél” (home institution).

A felhasználó első lépésben egy védett erőforráshoz fordul, azonban a Shibboleth webszerver-modulja átirányítja őt azonosítás céljából az identitás-szolgálta-



3. ábra

Liberty föderációs modell. Az autókölcsönző szolgáltatásait a légitársasághoz történő bejelentkezés után vehetjük igénybe



4. ábra
Shibboleth föderációs modell.
A szaggatott vonalak HTTP átirányítást jelölnek.

tóhoz. Azonosítás után az IdP kiállít egy SAML Assertion-t, amelyet (a böngészőn keresztül) eljuttat az SP-nek. Ezen a ponton a felhasználó azonosítottnak tekinthető.

Az autorizációs szakaszban az SP (az igazolásban található tranziens azonosító alapján) adatokat kér a felhasználóról. Mivel az adatcsere során személyes adatok utaznak, az IdP-nek lehetősége van arra, hogy tartalomszolgáltatónként, vagy akár felhasználónként *attribútum kiadási szabályzatot (Attribute Release Policy, ARP)* definiáljon. Az SP a kapott adatok és az erőforráshoz tartozó attribútum elfogadási szabályzat (Attribute Acceptance Policy, AAP) alapján engedélyezi vagy megtagadja a hozzáférést.

Mivel a Shibboleth általában tranziens azonosítókat használ, legjellemzőbb alkalmazási területei azok, ahol nem szükséges a felhasználó pontos kilétét megállapítani, hanem valamilyen jellemző csoporthoz tartozás alapján (például tanár egy bizonyos intézményben, hallgató egy adott kurzuson stb.) engedélyezzük a hozzáférést. Tipikusan ilyen terület lehet az e-learning illetve a hozzáférés olyan elektronikus gyűjteményekhez, melyek előfizetői nem az egyes felhasználók, hanem intézmények.

Az autorizációra szolgáló attribútumok használatának feltételeit a föderációs szerződés szabályozza (jogi eszközökkel). A Shibboleth-ben lehetséges ugyan állandó azonosítót is használni, azonban ekkor tisztázni kell, hogy ez milyen – a felhasználó privát szféráját érintő – adatvédelmi kérdéseket vet fel.

6. Összefoglalás

Az autentikációs és autorizációs infrastruktúra lényege, hogy az azonosítási és jogosultság-ellenőrzési feladatokat az alkalmazásoktól elkülönítve, szabványos illesztési módszerek felhasználásával végezzük.

Ilyen infrastruktúra létrehozásának akkor is lehet létjogosultsága, ha egyetlen intézményen belül használjuk, mivel a Single Sign-On egyszerűsíti a felhasználó számára az autentikációt, és megfelelően alkalmazva, magát az intézményi informatikai biztonságot is növelheti.

Várhatóan egyre több olyan projekt indul majd, melyben több intézmény közösen használ erőforrásokat. Ilyen esetekben a föderált identitás-menedzsment jelentősen csökkentheti a felhasználókhoz kapcsolódó költségeket.

Irodalom

[1] Lightweight Directory Access Protocol, RFC 3377, http://www.rfc-editor.org/rfc/rfc3377.txt
[2] PubCookie: http://www.pubcookie.org/docs/how-pubcookie-works.html
[3] OASIS Security Services Technical Committee: Security Assertion Markup Language (SAML) Schema and Specifications, http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
[4] Liberty Alliance: http://www.projectliberty.org/
[5] Shibboleth: http://shibboleth.internet2.edu/

Személyes adatok védelme és az AAI rendszerek

dr. Rátai Balázs

Informatikai- és Kommunikációs Jogi Kutatóintézet, Pécs
balazs.ratai@carneades.hu

A személyes adatok védelméhez való jogot az Alkotmány 59. paragrafusa rögzíti. Az Alkotmánybíróság a személyi szám alkotmányellenességét kimondó 15/1991-es határozatában aktív személyiségvédelmi jogként értelmezte az adatvédelemhez való jogot és leglényegesebb tartalmát abban határozta meg, hogy az emberek külső kényszerektől mentesen saját maguk jogosultak rendelkezni személyes adataik feltárásáról és felhasználásáról.

A személyes adatok kezelésének legfontosabb törvényi kereteit ma az 1992. évi LXIII. tv. határozza meg. Ebben a törvényben került meghatározásra, hogy mi számít személyes adatnak, valamint az, hogy milyen kötelezettségekkel jár az, ha valaki mások személyes adatait kezeli.

Az AAI rendszerek üzemletetése alapvető céljuknál fogva személyes adatok kezelésével jár együtt, ezért egy AAI rendszer létrehozásakor már a rendszertervezési fázisban érdemes foglalkozni azzal a kérdéssel, hogy az adatvédelmi előírásokat miként tudja majd teljesíteni az AAI rendszer üzemeltetője.

Az AAI rendszerek által kezelt személyes adatok három nagyobb csoportba oszthatók:

A) autentikációs adatok (többnyire természetes személyazonosító adatok),
B) autorizációs (jogosultsági) adatok,
C) a rendszer működése során keletkező adatok.

A három adatkör közül az első azokat az adatokat takarja, amelyek lehetővé teszik a felhasználók személyének azonosítását, azaz a „Ki a felhasználó?” kérdésre adnak választ.

Az autorizációs adatok azt a kérdést válaszolják meg, hogy mire jogosult az adott felhasználó.

A harmadik csoport pedig azon adatokat takarja, amelyek az AAI rendszerek működése során keletkeznek és az adatvédelmi törvény személyes adat meghatározásából adódóan személyes adatnak tekintendők. Az alábbi táblázat néhány példát tartalmaz a három adatkörbe sorolható személyes adatokra vonatkozóan.

Az AAI rendszerek tekintetében az adatvédelmi szabályozás által támasztott adatvédelmi követelmények és ezek teljesítésének hogyanja természetesen az AAI rendszer által kezelt személyes adatok körétől, mennyiségétől függ és nyilvánvaló összefüggésben áll azon szolgáltatások sajátosságaival, amelyek igénybevételét az AAI rendszer segíti. Ebből adódóan nagyon nehéz általánosságban meghatározni azt, hogy milyen módon kerülhető el a jogosulatlan adatkezelés.

Ennek ellenére érdemes néhány ökölszabályt szem előtt tartani egy AAI rendszer létrehozása és üzemeltetése során:

A) Törekedni kell arra, hogy minél kevesebb személyes adat tárolására és továbbítására kerüljön sor.
B) A rendszer működése során keletkező személyes adatok tárolására a lehetőségekhez képest egyáltalán ne, vagy csak rövid ideig kerüljön sor.
C) Az autentikációs és autorizációs adatok kezelésének szükségességét rendszeres időközönként felül kell vizsgálni.

Autentikációs adatok	Autorizációs adatok	Másodlagosan keletkező adatok
– név	– igénybe vehető szolgáltatások	– igénybevett szolgáltatás
– lakcím	– egyéb olyan jellemzők, amelyek a szolgáltatás igénybevételére való jogosultságot megalapozzák	– szolgáltatás igénybevételének időpontja
– életkor		– szolgáltatás igénybevételének helye
– azonosító		– szolgáltatás használatának időtartama