Debreceni Egyetem

Informatika Kar

Szövetségi (Federated) Azonosítás

Témavezető:
Prof. Dr. Pethő Attila
egyetemi tanár, dékán, tanszékvezető

Készítette:
Perge Zoltán
Mérnök Informatikus (B.Sc)

Debrecen
2009

Tartalomjegyzék

Bevezetés 3
A szövetségi azonosítás 4
Üzleti környezet 5
A vállalat leépítése 6
Vállalati újraszerveződés 6
Magas szintű példa az újra-csoportosításra 7
Üzleti modellek a szövetségi azonosításra 9
Példák a szövetségi azonosítás menedzsment alkalmazhatóságára vállalati fejlődésben 10
A kapcsolat – Bizalom és biztosítás 14
Szövetségi példa 16
Szövetségi azonosítás menedzsment architektúra 19
Háttér a federációhoz 20
Architektúra áttekintés 21
Szerepek 22
Identitásszolgáltató - IdP 23
Tartalomszolgáltató – SP 23
Azonosítási modellek 24
Megosztott 24
Különálló 25
Azonosítási attribútumok 26
Bejelentkezési adatok 27
Tranzakció attribútumok 28
Profil attribútumok 29
Szolgáltató-specifikus attribútumok 30
Bizalom 30
Transzport 31
Üzenet 32
Token 32

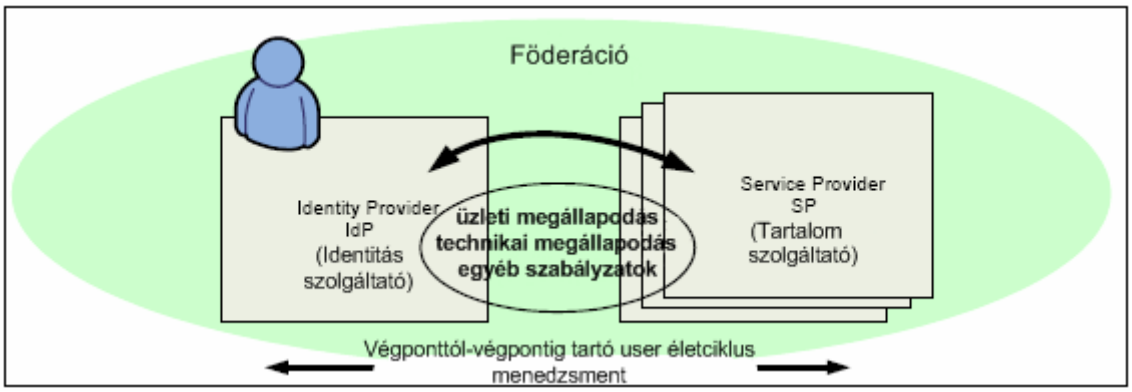
Szövetségi protokoll 32
Szabványok és törekvések 32
SSL/TSL 33
Security Assertion Markup Language (SAML) 33
A SAML története 34
A SAML építő elemei 35
A SAML anatómiája 36
SAML Assertion 36
SAML Protokollok 38
SAML Bindingok 41
SAML Profilok 43
SAML biztonság 44
Shibboleth 44
WS-Federation 45
Föderációs Single Sign-on 45
Push és Pull SSO 46
Account összekapcsolás 46
Where Are You From? (WAYF) 49
Session menedzsment és hozzáférési jogosultságok 50
Kijelentkezés 50
Bejelentkezési adatok eltakarítása 51
Globális good-bye 51
Account szétkapcsolás 52

Bevezetés

A témám a Szövetségi azonosítás, azon belül pedig a szövetségi azonosítás menedzsmentet, a szövetségek (nagy)vállalati környezetét, továbbá a vállalatok jövőjét, szövetségi azonosításból származó előnyei és az elvárásokat szeretném vizsgálni. Természetesen igyekszem még bemutatni a Szövetségek alapvető fogalmait és technológiáit. Választásom azért erre a témakörre esett, mivel saját szakomon belül (Mérnök Informatikus) a Vállalati Információs Rendszerek szakirányon folytatom tanulmányaim és itt már többrétű betekintést nyerhettem a vállalatok rendszerébe és a menedzsment tárgykörbe (Termelés menedzsment, Karbantartás menedzsment illetve Emberi-erőforrás menedzsment). Igyekezem az itt szerzett ismereteimet használni, bővíteni. Sajnos magyar nyelvű dokumentum ebben a témakörben igen elenyésző számban van, munkám során tehát főként külföldi forrásokra, irodalmakra támaszkodom. A következőkben az üzleti környezetet, a vállalatok jelenlegi fejlődési tendenciáit vizsgálom. Az üzleti környezet melyet, a növekvő alkalmazkodóképesség hajt, egyre nagyobb méretekben és egyre magasabb szinten lesz együttműködő a társaival, akikkel tranzakciókat folytatnak az új típusú üzleti folyamatok részeként.

A szövetségi azonosítás

A Szövetségi azonosítás technológiát globálisan együttműködő online üzleti azonosítási célokra, kapcsolatok vezetésére és cégek közti rokonsági alapú üzleti modellek létrehozására használják. Az ötlet lényegében nem új, minthogy vannak valós világbeli modelljeink az egyének szövetségi azonosításra – az útlevél nemzetközileg használható a személyazonosság igazolására; a bank kártya a tulajdonos bankszámlájáért kezeskedik; a vezetői engedély pedig a személy azon képességét igazolja, hogy tud gépjárművet vezetni és szintén használható személyazonosításra.



1. ábra – Szövetségi azonosítás menedzsment

Szövetségi azonosítás menedzsment alapjai az üzleti-, technikai megállapodások és szabályzatok melyek lehetővé teszik a cégeknek, hogy együttműködjenek az megosztott azonosítás menedzsment megoldásokkal. Ezáltal a cégek csökkenthetik az azonosítás menedzsment költségeiket és nagyobb felhasználói élmény[1] érhető el. Felhasználva a hordozható azonosító ötletét, ezáltal egyszerűsítve a felhasználók adminisztrációját illetve a biztonság és bizalom kezelését a szövetséges üzleti kapcsolatokban. Az adminisztráció és az életciklus management leegyszerűsödése a föderációban a következő eredményekhez vezettek:

- Az azonosítás menedzsment költségek csökkenthetők mivel a cégeknek nem kell többé a *felhasználók* és *azonosítóik* kezelésével foglalkozniuk, - mivel ez nem a hatáskörük – beleértve az adminisztrátorok delegálását mely sok jelenlegi első-generációs föderációs próbálkozás tartalmazott. A cégeknek kezelniük kell az

[1]**User Experience** - Így nevezzük azokat a benyomásokat, élményeket, amiket egy felhasználó egy termék vagy rendszer használata során szerzett. Forrás: http://www.fatdux.com/hu/what/what-is-ux/

adatokhoz való hozzáférést, viszont felhasználói accountokat és az ahhoz tartozó adatokat nem.

- A felhasználói élmény azáltal növekszik, hogy a felhasználó könnyedén navigálhat a web-oldalak között miközben a globálisan bejelentkezve marad.
- A végponttól-végpontig tartó biztonsági és bizalmi lehetőségeket hasznosítja a federáción belüli vállalatok-közti alkalmazás integráció.

Az integráció azért egyszerűsödhet, mert van egy közös út a hálózati identitásokhoz a cégek között vagy az alkalmazások között. A szervezetek olyan üzleti stratégiákat valósíthatnak meg, amelyek befolyásolják a szerves piacot és az ügyfelek számának növekedését azáltal, hogy kiküszöbölik a súrlódást, melyeket az összeférhetetetlen azonosítás- és biztonság menedzsment megoldások okoztak a cégek között.

Üzleti környezet

Ma a cégek igény szerinti fejlődést folytatnak azáltal, hogy az üzleti modelljüket a szerint fejlesztik, ami szükséges az érték-, és keresletnöveléshez az új termékeik és szolgáltatásaik iránt. Ebben a fejlődésben a vállalatok tipikusan afelé haladnak, hogy egy olyan céggé váljanak amely kulcs üzleti partnerekkel, szállítókkal és ügyfelekkel gyorsan és rugalmasan reagál mindenféle vevői igényre, piaci lehetőségre vagy külső fenyegetésre. Az ilyen vállalatok (igényekhez alkalmazkodó vállalatok) a következő kulcs tulajdonságokkal rendelkeznek:

Érzékeny Képes dinamikusan reagálni, az igényekben, szállításban, árképzésben, munkaerőben, versenyben és tőke piacon bekövetkező hirtelen változásokra.

Variálható Képes átalakítani a folyamatait és költség struktúráját, hogy csökkentse a kockázatot miközben fenntartja a magas termelékenységet és anyagi kiszámíthatóságot.

Összpontosított Képes koncentrálni a fő hatáskörére és azt elkülöníteni, szem előtt tartva az alkotórészek szükségleteit.

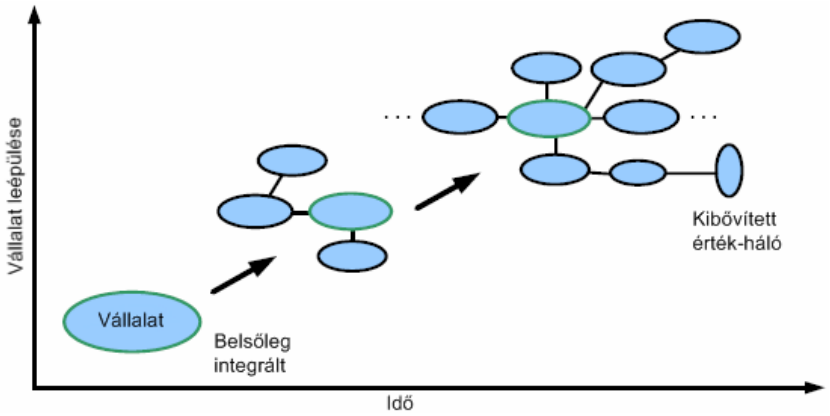
Rugalmas Képes kezelni a változásokat és külső fenyegetéseket miközben következetesen megfelel az alkotórészek szükségleteinek.

A folyamatban, hogy igényekhez alkalmazkodó vállalattá váljanak, a cégek sok változáson fognak keresztül menni. A vállalatoknak a leépítés és újra egyesülés útja új lehetőségeket és kihívásokat nyit meg.

A vállalat leépítése

A vállalatok leépülnek és partnerekből, szállítókból, ügyfelekből és versenytársakból álló kibővített érték-hálókká szerveződnek újra, hogy növeljék a termelékenységet és a rugalmasságot – a nem-létfontosságú folyamatok mellőzésével, csak a stratégiai, fő folyamataira fókuszálva. (lásd: 2. ábra)

A leépítést a nyílt szabványok és szolgáltatás központú architektúra adaptálása és fejlődése gyorsítja – a leépítés fokozott sebességet és kifinomultabb színvonalat mutat a globálisabb méretekben.



2. ábra: Vállalati leépülés

A fő mozgatórugó a változás mögött a technológia egyre növekvő átható természete, a nyitott szabványok, globalizáció és az üzleti modellek és IT adottságok növekvő fúziói. A növekvő együttműködés nagyobb üzleti jutalommal jár, de nagyobb üzleti rizikóval is, alapjaiban új üzleti döntéseket és biztonsági modellt igényel. Ahogyan a vállalatok haladnak a leépítés vonala mentén az igény, hogy rugalmasan összeszerkesszék és újraszervezzék az üzleti rendszereiket szükségszerűen nő – a vállalat újraszerveződik.

Vállalati újraszerveződés

Ahogy a komponensek és a szolgáltatások különválnak a vállalattól, a lehetőség, hogy újraszervezzék őket - a dinamikus és változó üzleti modell támogatásának érdekében -

egyre nő. A piac fokozatosan egy ilyen stratégiára vált. Ez az elképzelés az újraszerveződésre vagy integrációra, jól tükröződik a Szolgáltatás központú architektúra (Service Oriented Architecture, SOA)[2] stratégiában.

A SOA egy megközelítés olyan integrációs architektúrák meghatározására mely egy szolgáltatás elgondolásán alapul. A hatékony, igényekhez alkalmazkodó környezet kialakításához szükségesek üzleti és infrastrukturális funkciók szolgáltatásokként jelennek meg. Ezek a szolgáltatások a rendszer építőelemei.

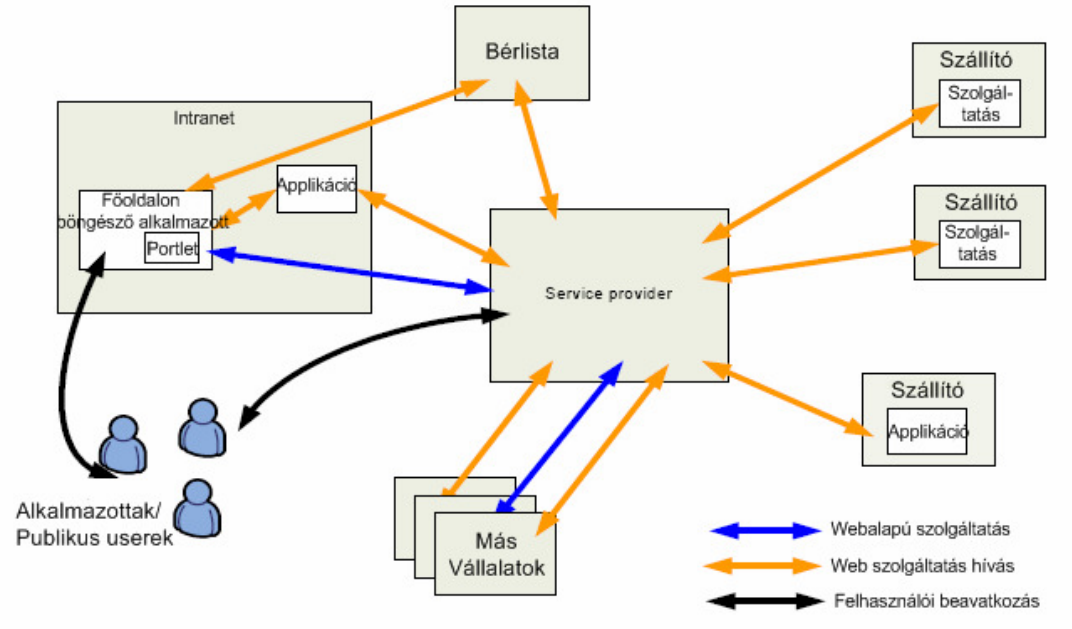
A SOA Web szolgáltatásokat használhat, elosztott rendszerek rugalmas és együttműködő szabványainak halmazaként. A SOA és a Web szolgáltatások között erős udvariassági jelleg van. A szoftver komponensek és Web szolgáltatások megfelelő pozícionálása a flexibilitást segíti elő, a jól definiált üzleti-szintű koncepciók, és a mechanizmus pedig az üzleti rendszerek újra szervezését.

Az üzleti folyamatok, ahogy ma megszokott, teljesülnek azáltal, hogy integrálják a felhasználói tapasztalatokat többrétű user interfészeken keresztül, amit az alkalmazásokat nyújtó Web szerverek reprezentálnak. Ma ez nagymértékben navigálja a Webet, de ahogy a portálok egyre áthatóbbá válnak, és a tartalmaik terjednek az Interneten, a felhasználói integrációt a federált egyszeri bejelentkezéssel (F-SSO) oldható meg. Ez az átlátható-, vagy user interfész integráció. A jelentős része a szövetségi azonosítás menedzsmentnek, a vállalatok-közti integráció és a felhasználó interfész integráció kombinációja.

Magas szintű példa az újra-csoportosításra

Egy olyan világban ahol egyre több és több szolgáltatás lesz elérhető a technológiának köszönhetően, beleértve olyan területeket ahol szükséges a rendkívül privát és érzékeny információ cseréje, a jelenlegi reaktív megközelítése az erőforrás (szolgáltatás) felhasználásnak nem elégíti ki egy valós-idejű, gördülékenyen csoportosuló szolgáltatás elvárásait mely optimálisan követni a változó piaci feltételeket.

[2] A **szolgáltatásorientált architektúra** (service-oriented architecture, SOA) különböző *üzleti* folyamatok integrálásának keretrendszere, és azt kiszolgáló informatikai infrastruktúra. Lazán kapcsolódó biztonságos, és szabványos komponensek - szolgáltatások -, amelyek újra felhasználhatók, újra kombinálhatók a folyamatok folytonos változásának, megújulásának megfelelően. - http://hu.wikipedia.org/wiki/Szolgáltatásorientált_architektúrák



3. ábra: A vállalatok újracsoportosulása összetett érték-hálóvá megsokszorozza a kapcsolatokat

A 3. ábra néhány integrációs pontot mutat be, amelyeket irányítani kell a szolgáltatások újra csoportosításának részeként, hogy támogathassák az új vagy már meglévő üzleti folyamatokat. Egy cég (az ábrán Intranet) *kiszervezi* a telekommunikációs és azzal kapcsolatos szolgáltatások részleg adminisztrációját (egy tartalomszolgáltatóhoz, Service Provider) és a bárszámfejtési részleget (Bérlista). Az tartalom szolgáltatónak viszont vannak hasonló kapcsolatai más ügyfelekkel, illetve a saját szállítóival. Megjegyzendő, hogy a Service Provider szintén kiszervezi a bérszámfejtést a Bérlista entitáshoz.

Ilyen kapcsolatok manapság több vállalatnál is léteznek, de nehéz feladat ezeket implementálni, testre szabni, fenntartani. Például egy üzleti folyamat, melyet szervezeti tartományokon keresztül kell megosztani, olyan problémákat vet fel, mint például a vállalati határokon keresztüli munkafolyamat. Az adminisztrációs szolgáltatónak magába kell gyűjtenie a szállítói által nyújtott szolgáltatásokat, egyesített szolgáltatások egy egybefüggő halmazába, mellyel, cserébe ellátja annak ügyfeleit. Ezen kívül a szállítónak gondoskodnia és garantálnia kell azt, hogy az információ biztonságos, szegmentált és bizalmas az ügyfelek között. A szállítóknak egymással is kell kommunikálniuk az alkalmazottak érdekében, fenntartva a titoktartást. A szállítónak ismernie kellhet a felhasználóit, akik számosak lehetnek.

A komplex dinamika és kollektív magatartás megértése és irányítása egyre fontosabbá válik, hogy elkerülhető legyen a rendszer instabilitása és, hogy előkészítse a terepet a globális és lokális optimalizálásnak. Egy alapjaiban új megközelítést kell implementálni, hogy biztonságos alapot szolgáltasson az igényeknek megfelelővé alakuláshoz, mely magában foglalja a föderációt és az elhatárolódást is.

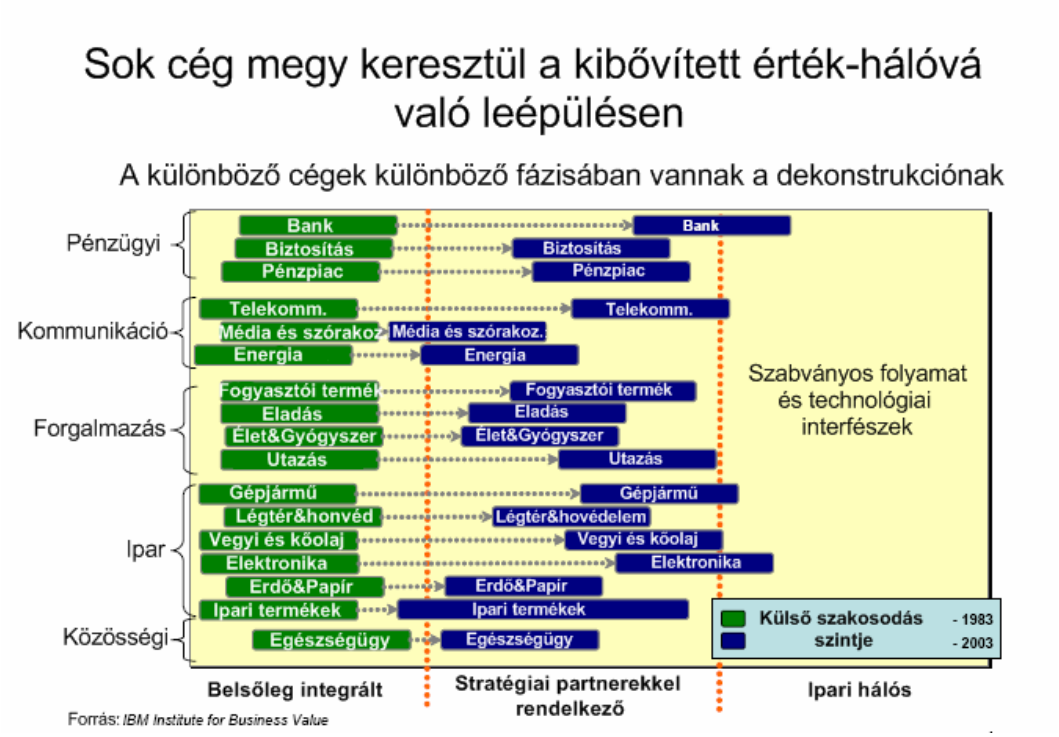
Tehát az interakcióknak, melyeknek eleget kell tenniük az új üzleti folyamatok elvárásainak, keverékei lesznek az alkalmazás-alkalmazás és felhasználói interakcióknak, melyek igénylik a szövetségi azonosítás menedzsment képességeinek teljes tárházát, hogy kezelhessék az azonosítás, bizalom és biztonság problémáit.

Üzleti modellek a szövetségi azonosításra

Ebben a részben, néhány lehetséges példát mutatok be melyek tükrözik a változó üzleti környezet kihívásait, továbbá a szövetségi azonosítás menedzsment tárgyköréhez is tartoznak. Annak érdekében, hogy a példák relevánsak legyenek a cégekre, vállalatokra és hatóságokra nézve, a példák öt különböző szektorból származnak.

Pénzügyi	A pénzügyi szektort a banki, pénzpiaci és a biztosítási részlegek reprezentálják.
Kommunikáció	Ehhez a szektorhoz az energia, a média és szórakoztatás és a telekommunikáció tartoznak.
Forgalmazás	A fogyasztói termékek tartoznak a szektorba.
Ipar	Az ipari szektorba a légtér és honvédelem, gépjármű és vegyipar, kőolaj és elektronika tartoznak.
Közösségi	A szektort az oktatás, kormányzás és egészségügy és élettudományok képviselik.

Először nézzük meg melyik fázisban tartanak a különböző szektorok a dekonstrukciós skálán.



4. ábra: A cégek különböző fázisaiban vannak a dekonstrukciónak – Forrás: IBM Institute for Business Value

Amint látható napjainkban a legtöbb cég a stratégiai partnerekkel rendelkező kategóriában vannak. Ebben a kategóriában az üzletek közt megosztott interfészek egyediek és nem újrafelhasználhatóak. Idővel az ipari hálós (kibővített érték-háló) fázisba kerülnek, ahol az interfészeket szabványok vezérlik a folyamatok, technológia és végül emberek egyenletes átmenetével. Ez a lépés a szövetségi azonosítás menedzsment fő mozgatórugója. Mivel a szektor iparágai különböző stádiumában vannak a dekonstrukciónak, így a szövetségi azonosítás menedzsment alkalmazásának sürgőssége eltérő. A bank, gépjárműgyártás, utazás és elektronika vannak az első helyeken a fejlődésben.

Példák a szövetségi azonosítás menedzsment alkalmazhatóságára vállalati fejlődésben

1. Egyesülés és felvásárlás

   Ilyen esetben a cég növekedési stratégiája a más cégekkel való egyesülésen illetve azok felvásárlásán alapszik. Ekkor a siker kulcsa az, hogy milyen gyorsan tudják a cégek az IT infrastruktúrájukat összekötni a másikkal, ezáltal nyerve új ügyfélkört. Ilyen esetekben az ügyfelek azonosítás menedzsmentje az egyik legkomplexebb probléma, ahelyett, hogy a megszerzett ügyfeleknek külön fiókot kellene létrehozni

egy a szövetségi azonosításon alapuló integrációs stratégia egyszerűsítheti a felhasználói élményt. Így a két cég felhasználói könnyedén elérhetik a másik cég erőforrásait, szolgáltatásait. Az egyesült cégek identitásainak federációja gyors és akadálymentes ügyfél integrációt biztosít.

2. Cégek közti együttműködés

   Több nagy cégnek vannak saját független üzleti egységeik, akik szeretnék fenntartani a kapcsolatot saját ügyfeleikkel. Ennek okai lehetnek a szervezeti struktúra, politikai vagy a versenytársak. Egy nemzetközi termelő cégnek lehetnek regionális képviseletei Amerikában, Európában, Ázsiában stb. és e képviseletek alkalmazottainak szüksége lehet a másik képviselet erőforrásaira. A szövetségi azonosítás menedzsment lehetővé teszi az üzleti egységeknek, hogy fenntartsák a függetlenségüket és rugalmas utat biztosít az adatok, erőforrások megosztására a vállalatok között.

3. Vásárlói bázis növekedése

   Egy olyan cégnek, amelynek a terjeszkedési stratégiája azon alapul, hogy megszerzik az új ügyfelek igényeit ez által megnyerve őket, vagy olyan cégekkel társulnak, amelyeknek meg akarják szerezni az ügyfeleit. Például egy pénzügyi szolgáltató társul egy mobil távközlési szolgáltatóval (akinek milliónyi előfizetője van), hogy elektronikus számlázási szolgáltatást nyújtson az ügyfeleinek, papíralapú helyett. Az ösztönzés a mobil szolgáltatónak ebben a társulásban az, hogy a nem létfontosságú kiadásait csökkentheti azáltal, hogy a számlázási feladatokat kiszervezi a pénzügyi szolgáltatóhoz. Cserébe a mobil szolgáltató 5 % engedményt ajánl az új e-számlázási szolgáltatásra előfizető ügyfeleknek. Ezen társulással a pénzügyi szolgáltató egy millió új ügyfélre tett szert, akik az új szolgáltatás lehetséges előfizetői. A szövetségi azonosítás menedzsment lehetővé teszi a pénzügyi szolgáltatónak, hogy új ügyfélbázisokat érhessen el, akiknek már meglévő saját identitásuk van. (A különböző identitás menedzsment megoldásokkal rendelkező cégek közti integrációt megoldva.)

4. Kiszervezett szolgáltatások

   Az alkalmazottak önkiszolgálása elsődleges kezdeményezés több vállalatnál, akik csökkenteni kívánják a felhasználók kezelésének költségeit. Több szervezet

kiszervezi a nem kritikus kompetenciákat külső (harmadik fél) szolgáltatókhoz (Ilyenek lehetnek emberi erőforrás, magán nyugdíjpénztár, egészségbiztosítás, utazás stb.) A vállalati intranetes portál segítségével elérhetők ezek a külső szolgáltatók, továbbá így a vállalatnak csak a kiszervezett szolgáltatások adminisztrációját kell ellátnia. Azonban mivel az alkalmazottakat nem tudják közvetlenül hozzákapcsolni a szolgáltatókhoz, így szükséges információs szolgálatot (help-desket) fenntartani az alkalmazottak iktatásához a magánnyugdíj-pénztár, egészségbiztosítás és bérlista szolgáltatásokat tekintve. A munkáltatók jelentős összeget fordítanak e szolgáltatások adminisztrációs költségeinek megtervezésére, de végül mégis a vállalatnak magának kell adminisztrálnia ezeket a szolgáltatásokat vagy alkalmaznia kell ügyfélszolgálati személyzetet.

A szövetségi azonosítás menedzsment lehetővé teszi az alkalmazottaknak, hogy elérjék és kezelhessék az adataikat a különböző tartalomszolgáltatók Web oldalain, az alkalmazotti portálon való bejelentkezést követően. Egy már meglévő portál használata egyszerűsíti a felhasználói élményt és lehetővé teszi, hogy a felhasználó elérje a különböző szolgáltatók weboldalait anélkül, hogy az üzleti partnereknél regisztrációt vagy hitelesítést igényelne. A munkáltató csökkentheti az alkalmazott támogatás- és adminisztrációs költségeket azáltal, hogy a dolgozók közvetlen elérhetik a szolgáltatókat.

5. Tartalomszolgáltató automatizáció

Egy nagyobb tartalom szolgáltatónak, aki alkalmazottak magán nyugdíjpénztári accountjait kezeli, az ügyfelek alkalmazottainak felhasználói életciklus kezelése jelentős költségeket jelent. Ezek a költségek az ügyfelek alkalmazottainak account regisztrációjából és kezeléséből, a jelszavak kezeléséből illetve ügyfélszolgálat fenntartásából (aki foglalkozik a felhasználók elfelejtett jelszavainak és bejelentkezési adatainak problémájával) erednek.

Tételezzük fel, hogy $ 20 egy ilyen új jelszó kérő hívás, és adott egy tartalomszolgáltató, aki 100 ügyféllel rendelkezik, és minden ügyfélnek átlagosan 10000 alkalmazottja van. Ha ezeknek csak a negyede évente egyszer elfelejti a jelszavát, az 5 millió dolláros kiadást jelent az account és jelszókezelésben. A tartalomszolgáltató jelentősen érdekelt a szövetségi modellre váltásban ahol a szolgáltató felhasználja az alkalmazottak hitelesítését az egyesített portálon, így

hozzáférve a szolgáltatásaikhoz. Ebben a modellben a munkáltató (ügyfél) felelős a felhasználóinak és jelszavainak kezeléséért (amely egyébként is a feladatuk, tehát nem jelent plusz költséget), a tartalomszolgáltató pedig az ügyfeleire hárítja a felhasználói adminisztráció költségeit. Ez a megközelítés az alkalmazottak számára is kedvező mivel nem kell több helyre is regisztrálnia illetve több jelszót fejben tartania, hogy kezelhesse a magán nyugdíjpénztári és egészség biztosítási adatait.

6. Portál alapú integráció

   Az internet alapú szolgáltatók új generációja, a vállalatoknak és cégeknek kínál szoftver-mint-szolgáltatás megoldásokat. Ilyen szolgáltatók például WebEX, Salesforce.com, Travelocity.com és így tovább. Ezek a szolgáltatások lehetővé teszik, hogy a vállalatok hozzáférjenek Interneten hosztolt szolgáltatásokhoz anélkül, hogy az IT infrastruktúra költségeit magára kellene vállalnia melyet e szolgáltatások helyi kezelése jelentene. A szövetségi azonosításnak kritikus szerep jut ebben a rendszerben, mert lehetővé teszi a cégek alkalmazottainak, hogy különböző szoftver alapú szolgáltatásokat érjenek el a saját munkahelyi belépési azonosítóikkal. Miközben egyre több és több cég szervezi ki a nem létfontosságú üzleti szolgáltatásait, a szövetségi azonosítás menedzsment tölti be egy olyan identitás integrációs technológia szerepét mely segítségével a felhasználók akadálymentesen elérhetnek harmadik-személy által nyújtott szolgáltatásokat melyek lehetnek helyileg- vagy távolról hosztoltak.

7. Közigazgatási együttműködés

   A közigazgatásban nagy az igény a hatékonyságra és az együttműködésre. A folyamatok több kormányzatot, intézményt és hatóságot áthidalhatnak különböző régiókban, ahol szükséges az adatok megosztása, de politikai, intézményi vagy egyéb okokból nincs lehetőség az integrálódásra vagy egyesülésre. Az entitásoknak, a felhasználóik számára szükséges lehet a kormány-közi entitások erőforrásainak elérhetővé tétele. Például egy európai ország valamely hatóságának szüksége lehet lényeges információra egy személyt illetően egy másik ország adatbázisából, azonban ehhez szükséges lenne egy ország hatóságának a másik ország hatósági felhasználóit kezelnie.

A szövetségi azonosítás lehetővé teszi, hogy a hatóságok megőrizzék függetlenségüket és a saját felhasználóik kezelését, miközben egy flexibilis megoldást kínál az adatmegosztására a kormány-közi entitásoknak.

A kapcsolat – Bizalom és biztosítás

A szövetségi üzleti modell kijelöli a *bizalom körét*. A szövetségi modellben a szervezet, amely elérést szeretne biztosítani egy identitásnak, akit nem ellenőriz a szervezet saját belső biztonsági eljárása. Ehelyett a szervezet megbízik egy harmadik személy kijelentésében az identitást tekintve. Egy modell, amely rizikót és a bizonytalanságot visz, az üzleti tranzakciók bizalmasságába.

Egy szervezet nem hoz létre szövetségi üzleti modellt, ha nincs rálátása az üzleti partner identitás és hozzáférés kezelési rendszerébe és folyamataiba. A szervezetnek meg kell becsülnie az üzleti partnerekkel való együttműködés kockázatát és felmérni a partner üzleti folyamatait és ellenőrző eljárásait az 1) üzleti partner identitásigazolásra 2) üzleti partner akkreditációra 3) üzleti partner (jó) hírnevének megállapítására. Ezek a folyamatok biztosítják az átláthatóságot és minőségi értékelést adnak arról, hogy a harmadik fél identitás miként vonható be az üzleti döntésekbe a hozzáférés vezérlésről és a bizalmi kapcsolat szabályairól, melybe a szervezet belépni kíván az üzleti partnerrel.

Az üzleti partner identitásigazolása az a folyamat melyben ellenőrzik a leendő szövetséges üzleti partner fizikai identitását, mind az online üzleti kapcsolat létrejötte előtt és mikor már elkezdték a futásidejű tranzakciókat. Az identitásigazolás része a vállalat fizikai identitásának ellenőrzése – de ki is a vállalat?

- Létezik-e az adott néven törvényes vállalat?
- Az üzleti partner küldi a kérést?
- Az adott dolgozó jogosult erre a kérésre?

Amikor az adott fizikai identitást leellenőrizték, valamilyen online token-t bocsátanak ki az üzleti partnernek, ezután pedig összekapcsolják a vállalat adott fizikai identitásával. Az üzleti partner identitás ellenőrzés különböző módjai használatosak, beleértve:

- Önazonosítás
- Meglévő kapcsolat felhasználása
- Elektronikus vagy postai levélcím megerősítése
- Identitás ellenőrzés

Az üzleti partner akkreditáció, arra a kérdésre ad választ, hogy mit tudunk a cégről? Különösen, hogy mit várhatunk ettől a cégtől? Az akkreditáció egy jól meghatározott szabályzaton alapul, mely azt írja le, hogy milyen elvárásoknak kell egy partnernek megfelelnie. Egy föderációt kiépíteni akaró cégnek ki kell adnia egy ilyen szabályzatot, ugyanígy a partner cégnek is meg kell határoznia mely kritériumoknak, felel meg a saját IT infrastruktúrája. A két szabályzat illeszkedésének kiértékelése egy megbízható fél feladata, aki az üzleti akkreditációra szakosodott.

Példák a jellemzők típusára melyeket kiértékelnek az akkreditációs folyamatban:

- Hitelt érdemlő a vállalat?
- Jó hírnevű vállalatnak tartják a céget?
- A vállalatot elismerik a fontosabb szakmai szakszervezetek?
- A vállalat része a szövetségnek?
- A vállalat, belépési azonosítóit szabványosított és megbízható formában bocsátja ki?

A hírnév egy alternatív eszköze annak, hogy értékelhető kiegészítő információnak legyünk birtokában a vállalatról. A fő különbség a jó hírnév szolgálat és az akkreditáció között, hogy a hírnevet folyamatos alapon figyelik a vállalat viselkedési információi alapján. Másik különbség, hogy a hírnevet tipikusan egy független entitás figyeli, és nem foglalja magában az alany részvételét. A reputációmérésre napjainkban egy nyílt visszajelzés alapú mechanizmust használnak. A jó hírnév szolgálat általában egyszerű értéket határoz meg, melyet egy adott, könnyen érthető eljárás segítségével számít.

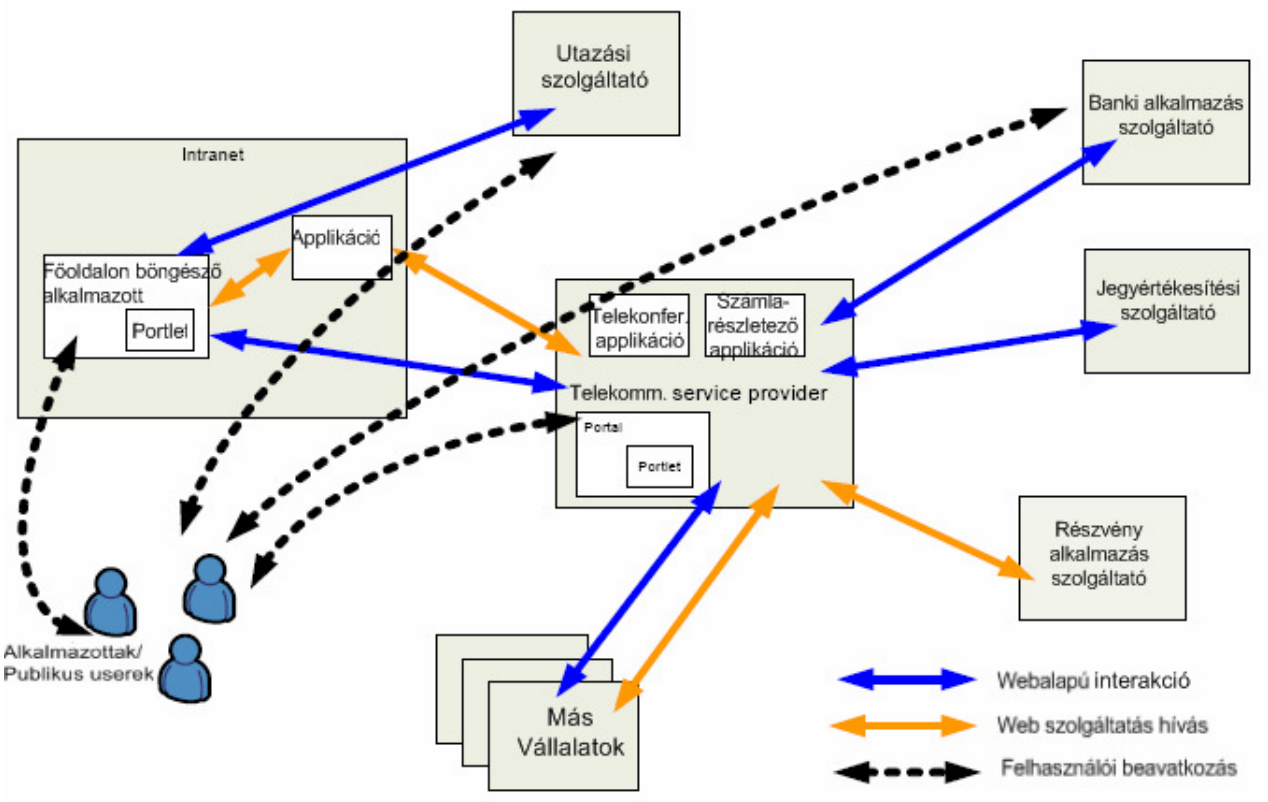
A szervezeteknek kritikus kihívásokkal kell szembesülni federációs modellben, a kapcsolat rizikófaktorainak meghatározásakor. Az üzleti partner identitás ellenőrzése, akkreditációja és hírneve alapvető szempontok, amelyek segítenek a cégeknek, hogy meghatározhassák a bizalom és biztosítás szintjét az üzleti partnereik identitás menedzsment megoldásaiban.

Szövetségi példa

A föderáció és a szövetségi azonosítás menedzsment potenciális előnyei legjobban egy példán keresztül mutathatók be. Tételezzük fel egy forgatókönyvet, a következő entitásokkal:

- Egy munkáltató NagyCég és egy alkalmazottja Első Alkalmazott
- Egy utazási szolgáltató, RBTravel
- Egy bank, RBBanking
- Egy részvény információs szolgáltató, RBStocks
- Egy felhasználó, Kiss József, aki azt interneten intézi ügyeit

Ezek a vállalatok kapcsolatban vannak egymással így létrehozva egy szolgáltatásokból álló értékhálót a végfelhasználóknak legyenek ők publikus userek vagy alkalmazottak.



4. ábra: Példa a federációs környezetre

NagyCég NagyCég egy nagyvállalat sok alkalmazottal. NagyCég, az alkalmazottainak több foglalkoztatással kapcsolatos szolgáltatást biztosít (egészségbiztosítás, magán nyugdíjpénztár, céges mobiltelefon előfizetés). Az alkalmazotti költségek csökkentése érdekében NagyCég kiszervezi ezeket szolgáltatásokat harmadik-fél

	szolgáltatókhoz. NagyCég felelős az alkalmazottak kezeléséért kezdve az account létrehozásától annak törléséig (elbocsájtás/nyugdíjazás/egyéb ok) természetes, hogy NagyCég ezeket a funkciókat magára vállalja, de felhasználja a kapcsolataiban a harmadik fél szolgáltatókkal.
Alkalmazott 1.	Egy tipikus NagyCég dolgozó. Hozzáférése van a tipikusan NagyCég által nyújtott (közvetített) szolgáltatásokhoz. Egyúttal Első úr kiegészítő szolgáltatásokat is igénybe vesz, melyeket harmadik fél szolgáltatók biztosítanak úgy, mint utazási szolgáltatások, NagyCég által szponzorált mobil telefon előfizetés, részvények utáni részesedés és online bankolás.
RBTravel	RBTravel utazással kapcsolatos szolgáltatásokat nyújt vállalatoknak, lehetővé téve repülőjegyek, vonatjegyek, autó bérlés és szállás rendelését és fizetését. RBTravel-nek megállapodása van a szolgáltatásokat igénybe vevő vállalatokkal, hogy bárki, aki a vállalattól navigál hozzájuk automatikusan kap egy accountot.
RBTelkom	Egy telekommunikációs tartalomszolgáltató, amely beszédalapú telefonszolgáltatásokat nyújt, továbbá van egy portálja ahol a saját- vagy üzleti partner felhasználók választhatnak a felajánlott szolgáltatások között, melyekhez az RBTelkom mint SSO-t biztosító identitás szolgáltató viselkedik. Ezen kívül RBTelkom-nak vannak olyan szolgáltatásai a portálon, melyek külső partner szolgáltatókhoz kapcsolódnak. RBTelkom tartalomszolgáltatóként viselkedik a nagyvállalatok – mint például NagyCég – számára.
RBBanking	Banki szolgáltatásokat kínál saját ügyfeleinek illetve RBTelkom ügyfeleinek a portálon keresztül.

NagyCég egyike az identitás szolgáltatóknak ebben a szövetségi kapcsolatban. Kezeli a felhasználói nyilvántartást, amely tartalmazza az információkat a saját alkalmazottairól. Felelős az alkalmazottai életciklus kezeléséért, kezdve az account létrehozásától egészen a törlésig/inaktivizációig.

NagyCég üzleti federációt köt egy utazási szolgáltatóval, RBTravel-lel aki szolgáltatásokat kínál NagyCég dolgozóinak. A RBTravel-nek kezelnie kell az információkat az

alkalmazottakról mivel ezek az adatok (utazási szokások, törzs utas információk) lényegesek RBTravel naprakész utas specifikus információ menedzsmentjéhez.

Első úr rendelkezik NagyCég accounttal, amellyel elérheti a NagyCég erőforrásait melyek a munkájához szükségesek. Az account alapja a meglévő munkaviszony. Ha Első úr szabadságra megy, felfüggeszthetik az accountját. Ha netalán máshol vállal munkát, akkor törlik az accountot.

Első úr, NagyCég alkalmazott lévén, rendelkezik egy szponzorált accounttal RBTravel-nél aki harmadik fél tartalomszolgáltatóként viselkedik. Az, hogy Első úr accountja szponzorált azt jelenti, hogy az account annak eredményeként jött létre, hogy Első úr NagyCég alkalmazott. Első úr elérheti az utazási információit a NagyCég alkalmazotti portáljáról. A portáltól egy hivatkozás mutat RBTravel Web portáljára, amely átirányítja Első urat RBTravel-hez annak érdekében, hogy elérje a cégen kívüli szolgáltatásokat és információkat. Szövetség nélkül Első úrnak külön hitelesítenie kell RBTravel-nél, hogy elérje accountját, annak ellenére, hogy már bejelentkezett NagyCégnél és az alkalmazotti portálon átirányították RBTravel-hez.

Egy federációs kapcsolatba lépéssel RBTravel csökkentheti a felhasználók kezelésének költségeit. Ennek zöme azáltal érhető el, hogy egyszeri bejelentkezést alkalmaznak, és nem közvetlenül kezelik Első úr bejelentkezési adatait, amely költséges része a felhasználói életciklus kezelésnek. Az, hogy NagyCég és RBTravel federációs kapcsolatot hoznak létre egyszerűsített SSO-val, Első úr szemszögéből azt jelenti, hogy egyszer kell csak bejelentkeznie NagyCégnél és elérheti az utazási információit újbóli hitelesítés nélkül. A szövetségi egyszerűsített SSO a két fél között (NagyCég és RBTravel) elősegíti a biztonságos és megbízható átvitelét a felhasználói azonosítókat és egyéb attribútummal kapcsolatos információkat (autorizációs szerepek, csoporttagságok, jogosultságok és attribútumok például azonosító, hitelkártya szám).

Az szükséges, hogy RBTravel részt tudjon venni az információ futásidejű cseréjében NagyCéggel, ez valamilyen NagyCégtől származó kijelentést (assertion) eredményez (megjegyzendő, hogy az információ csere nem igényel beavatkozást Első úrtól). Ezt a kijelentést RBTravel megbízhatónak találja és felhasználja Első úr egyedi azonosítására, a NagyCég által kiadott egyedi azonosító alapján. Ezen információ felhasználásával RBTravel képes lokálisan azonosítani és elérést biztosítani Első úr accountjához. Azonban NagyCégnek és RBTravel-nek is tárolnia kell információt Első úrról. Bizonyos attribútumok NagyCég

számára fontosak ilyenek a lakáscím és telefonszám, ugyanígy némely információ Első úrról sokkal inkább RBTravel-hez kapcsolható, ilyenek az utazási szokások. Ezen attribútumok segítségével jobban személyre szabhatja a felhasználói élményt.
A másik főszereplő ebben a példában RBTelkom, aki szolgáltatásait üzleti és egyéni előfizetőknek kínálja. Az üzleti előfizetéseknél általában nem foglalkozik egyénenként az alkalmazottakkal, a hitelesítés tekintetében egy felhasználóként kezeli mindet. Bizonyos szolgáltatások, mint a telekonferenciák előjegyzése nyilván csak vállalatok számára elérhető. A vállalatoktól továbbított attribútumok lehetővé teszik RBTelkom-nak, hogy jobban személyre szabják a felhasználói élményt.
Az egyéni ügyfeleknek saját accountjuk van a RBTelkom portálon. Az egyéni ügyfelek javára szolgálhatnak a partnerek szolgáltatás ajánlatai, melyek elérhetők portálról. A SSO segítségével elérhetők a szolgáltatások, mivel elegendő csak a RBTelkom portálra bejelentkezni aztán a partner hivatkozására klikkelni, majd további hitelesítés nélkül böngészni a partner szolgáltatásai között. Ilyen például a RBBanking, amely a banki szolgáltatásait SSO-val elérhetővé teszi a RBTelkom portálról, ugyanúgy ahogy RBTravel hirdeti az ajánlatait NagyCégnél.

Szövetségi azonosítás menedzsment architektúra

A federációs azonosítás menedzsment (FIM) segítségével a vállalatok és üzleti partnereik csökkenthetik az identitáskezelési költségeket, fejleszthetik a felhasználói élményt, erősíthetik a cég gyenge pontjait és mérsékelhetik a tranzakciók biztonsági rizikóit. A szövetségi azonosítás tárgyalásakor különböző probléma megoldási területére bonthatjuk:

- Web alapú egyszeri bejelentkezés – Federált Single Sign-on (F-SSO)
- Applikáció alapú Web szolgáltatás biztonság – Biztonságos Web szolgáltatások
- Identitás életciklus – Federált provisioning[3]

Dolgozatomban én csak az első területet vizsgálom meg részleteiben.

---

[3] Telekommunikációs körökben a **provisioning** kifejezés egy telekommunikációs szolgáltatás aktiválását vagy megváltoztatását jelenti. Ez maga a folyamat, a felhasználói igény jelzésétől az összes szükséges változtatás megtételéig (például adatbázisokba a változás bevezetése, kábel kihúzása, ügyfél számára berendezések átadása).

Felhasználó provisioningnek nevezzük a felhasználói objektumok és felhasználói attribútumok létrehozását, fenntartását és deaktiválását, mivel ezek egy vagy több rendszerben, könyvtárban vagy applikációban létezhetnek az automatizált vagy interaktív üzleti folyamatoknak köszönhetően.

Háttér a federációhoz

Egy federációs megoldás akkor sikeres, ha az ügyfeleknek, üzleti partnereknek és végfelhasználóknak egyszerű integrálódást tesz lehetővé a federációs üzleti partnerek között anélkül, hogy kapcsolatonként külön meg kellene oldani a processzek biztonságát és azonosítást. Sajnos, a jelenlegi implementációk a biztonság és azonosítási adatok kezelésére, gyakran arra kényszerítik a felhasználókat és vállalatokat, hogy saját maguknak kell kezelni a hozzáférést, bizalmat, adatátvitelt és identitás attribútumokat. Gyakran ez a teher eléggé keményen rányomja a bélyegét az adminisztrációs költségekre, mivel mindegyik vállalatnak külön kell kezelnie egy nagy és gyorsan változó identitás adatbázist. Az ilyen modell akadálya a szövetségek bevezetésének, és gyenge pont mind a felhasználóknak, mind a vállalatoknak.

A szövetségi technológia:

- Egyszerű mechanizmust biztosít az üzleti partnerek felhasználóinak azonosítására és validálására és akadálymentes elérést biztosít a védett Weboldalakhoz az adott Szövetségen belül
- Szabvány alapú végponttól-végpontig tartó bizalom és biztonság támogatása az alkalmazásoknak a vállalatok között
- A felhasználó menedzsment költséges részeinek (accountlétrehozás, jelszó menedzsment, felhasználói ügyfélszolgálat) átruházására egy üzleti partnerre, az Identitás szolgáltatóra

A federáció célja tehát egy dinamikus és akadálymentes erőforrás- és szolgáltatás integráció támogatása a szövetségen belüli vállalatoknak.
Egy szervezet általában csak akkor fog federációs modellre váltani, ha ki tudja használni annak előnyeit a rizikó ellenében melyet a harmadik félben való bizalom jelent. A szervezet nem fog csatlakozni a szövetséghez, ha a federációnak nincs ugyanolyan átlátható harmadik fél felhasználói életciklus menedzsmentje, mint saját magának. Tehát a szövetségi azonosítás életciklus menedzsment egy olyan megoldás mely azonos átláthatóságot biztosít a vállalati folyamatokban, lényegesen eltérő identitás menedzsment rendszerek esetén is.

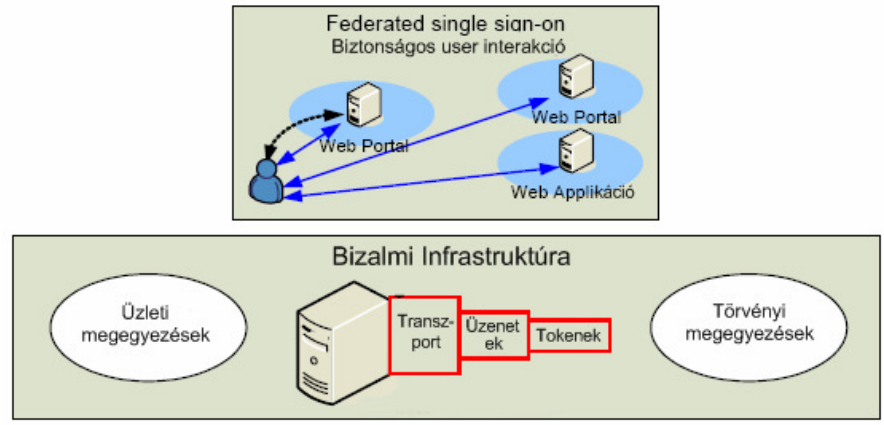
Architektúra áttekintés

A szövetségi kapcsolatok alapulhatnak, saját technológiákon melyekkel az üzleti partnerek kommunikálhatnak és együttműködhetnek. Általában a saját megvalósítás nem skálázható vagy alkalmazható több partner esetén. Ezen okból a szabvány és specifikáció alapú megközelítések nagy népszerűségre tettek szert. A szövetségek megkönnyítik a vállalatok integrálását.

Szövetségekbe lépés két jelentős funkciót könnyít meg:

- Problémamentes és biztonságos felhasználói interakció a szövetséges üzleti partnerek között (F-SSO)
- Problémamentes és biztonságos vállalati interakció, alkalmazás platform integráción keresztül (Web szolgáltatások biztonság menedzsmentje Szolgáltatás központú architektúráknak)

Ezek egy alapvető funkciót igényelnek a *bizalmi infrastruktúrát*. A bizalmi infrastruktúra nyújtja az üzleti partnerek közti üzleti és törvényes megegyezések műszaki ábrázolását és implementációját.



5. ábra: Bizalmi infrastruktúra

A szövetségi azonosítás menedzsmentre gyakran utalnak úgy, mint felhasználó által irányított, böngésző alapú vállalatok közti interakció. Azonban sokkal több haszna van, mint csak a *szövetségi single sign-on* (F-SSO). A szabványok és specifikációk, mint a SAML és a Liberty Alliance ID-FF specifikációk mind tartalmazzák a munkamenet (session) élet ciklus menedzsmentjét (egyszeri be/ki jelentkezés) továbbá az account összekapcsolást. Ezeknek a

technológiáknak köszönhetően egy partner végzi a hitelesítést, jelentős költséget levéve a vállalatok válláról.

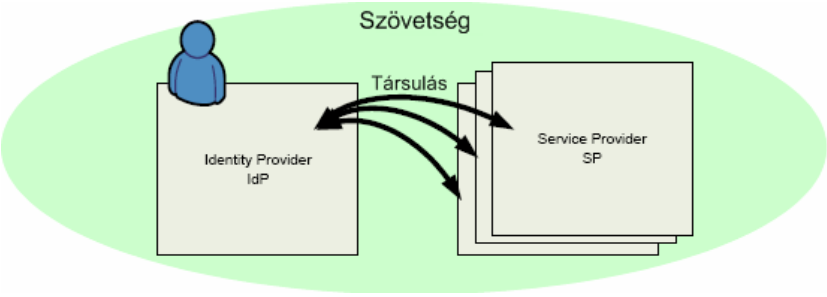
A bizalmi infrastruktúra konkrét implementációja, a *bizalmi szolgáltatás*. A bizalmi szolgáltatásra két megoldás rétegződik: a *Szövetségi Single Sign-On* és a *Web szolgáltatások biztonság menedzsmentje*.

Egy ilyen megoldás tervezéséhez, a következő területeket kell megismerni:

- Az azonosítás- és tartalomszolgáltató *szerep*eit: Annak a meghatározása, hogy ki a felhasználói azonosítási információ hiteles forrása.
- Identitás/attribútum *mapping* (leképzés): Azt jelenti, hogy mely attribútumokat osztunk meg továbbá a leképzésüket az üzleti partnerek rendszereiben.
- User accountkezelés: Eljárások a felhasználók azonosítási adatainak kezelésére, megegyezés a megosztott és függetlenül kezelt információkról.
- *Account összekapcsolás:* Eljárások az account összekapcsolás kezelésére, megegyezés a közös egyedi azonosítókról, melyeket összekapcsolhatnak a belső, helyi felhasználói identitással az tartalomszolgáltatónál. Ez a lépés tartalmazza az account szétkapcsolási eljárásokat is.
- *Bizalom:* A bizalom megteremtése jogi és szabályozási kérdés, azonban a bizalom megtartása technológiai kihívás. Eljárások a kapcsolatok/átvitel, az üzenetek és tokenek biztonságának biztosítására.
- A szövetségi protokoll profil(ok) kiválasztása: Az üzleti partnerek között használatos profilok meghatározása.

Szerepek

Egy szövetségen belül, az üzleti partnerek két szerepet játszhatnak: *Identity Provider* (Identitás Szolgáltató, IdP) vagy *Service Provider* (Tartalomszolgáltató, SP) esetlegesen mindkettő. Az identitásszolgáltató a hitelesítő fél, hitelesíti a végfelhasználót és kiállít egy identitást az usernek - valamilyen megbízható formában -, az üzleti partnerek számára. Azok az üzleti partnerek, akik szolgáltatásokat kínálnak, de nem viselkednek identitásszolgáltatóként, az tartalomszolgáltatók. Az IdP vállalja magára a felhasználói életciklus menedzsmenttel kapcsolatos problémákat. Az tartalomszolgáltató (SP) az IdP-re támaszkodik, hogy az kijelentsen a felhasználóval kapcsolatos információkat, és így az SP csak azon user attribútumokat kezeli melyek a saját maga számára fontosak.



6. ábra: Identitásszolgáltató és tartalomszolgáltató a szövetségi modellben

Identitásszolgáltató – IdP

Az IdP felelős az account létrehozásáért, beállításokért, jelszó kezelésért és az általános account kezelésért továbbá gyűjtőpontként vagy kliensként viselkedik a megbízható identitásszolgáltatókhoz. Egy szövetségi üzleti partner, aki a felhasználók IdP-jeként működik, megszabadítja a megmaradó üzleti partnereket annak a terhétől, hogy a felhasználóra vonatkozó ekvivalens adatokat kezeljenek. A nem IdP üzleti partnerek SP-ként viselkednek. Ezek a SP-k a bizalmi kapcsolatot használják az IdP-vel, hogy az IdP által egy felhasználóról kiadott tanúsítási információk elfogadják. Ez teszi lehetővé, hogy a vállalatok (tartalomszolgáltatók) az azonosítás és hozzáférés menedzsment költségeket átruházzák egy másik üzleti partnerre (az identitásszolgáltatóra) a federáción belül.

Tartalomszolgáltató – SP

A tartalomszolgáltatók védett tartalmakat szolgáltatnak a felhasználók számára. Általában nincsenek közvetlenül a felhasználókhoz kapcsolatos adataik, ezért nem szükséges a felhasználókat adminisztrálniuk sem.

A tartalomszolgáltató funkciói (a funkciók föderációs modelltől függően ezektől eltérhetnek):

- azonosított kapcsolat létrehozása az identitásszolgáltató segítségével (általában HTTP átirányítás használatával)
- az identitás szolgáltatótól kapott adatok értelmezése
- az identitás szolgáltatótól kapott adatok alapján meghatározni, hogy a felhasználó jogosult-e a művelet végrehajtására (**autorizáció**)

A tartalomszolgáltató kezelhet helyi információt a felhasználókról, még a szövetség kontextusán belül. Például, belépve egy szövetségi azonosítás menedzsment kapcsolatba lehetséges, hogy egy tartalomszolgáltató átadja az accountkezelést (beleértve a jelszó

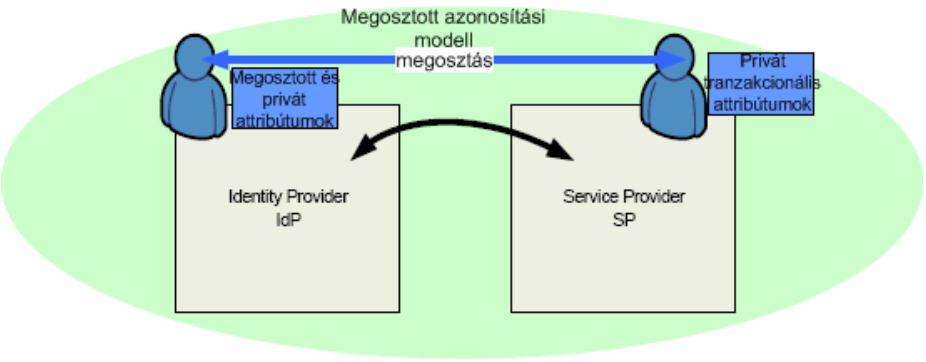
menedzsmentet) egy IdP-nek míg a SP a saját user-specifikus adatok kezelésére fókuszál (például SP oldali szolgáltatás-specifikus attribútumok és a személyre szabással kapcsolatos információ). Általában, az tartalomszolgáltató rábízza az azonosítás menedzsmentet az identitásszolgáltatóra, így minimalizálva az azonosítási követelményeket miközben változatlanul elérhetővé teszi a teljes tartalomszolgáltatói funkcionalitást.

Azonosítási modellek

A megosztott és különálló azonosítási modellek az azonosítási adat menedzsment természetére utalnak. A megosztott azonosítási adat menedzsment megosztott volta arra utal, hogy az azonosítási információt egy üzleti partner kezelheti (az IdP). A különálló pedig, hogy az információ ismétlődik, és külön kezelik az üzleti partnerek között.

Megosztott

A megosztott azonosítás a szövetségi üzleti interakciókban akkor lehet megfelelő mikor egy üzleti partner képes megbízni egy identitásszolgáltató által egy felhasználóról tett kijelentésben. Ebben a modellben a szövetség lehetővé teszi a felhasználónak (és a federációs üzleti partnereknek), hogy létrehozzanak egy közös egyedi azonosítót, amellyel utalhatnak a felhasználóra. Az azonosító alapján az identitásszolgáltató képes kezelni az user azonosítási adatait, és ezen információ hiteles forrásaként működik, a megbízható tartalomszolgáltatók számára.



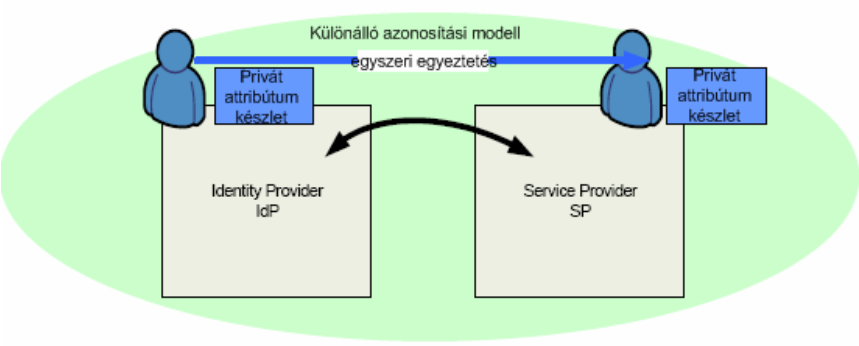
7. ábra: Megosztott azonosítási modell

Alapvető kérdés - figyelembe véve az azonosítás és attribútum kezelést az üzleti partnerek között – hogy milyen információk oszthatók meg és mik az előnyei a megosztásnak? A legoptimistább lehetőségként az IdP és SP minden információt megosztanak, ahogy az a 7. ábrán látható.

- A *bejelentkezési adatok megosztása* az identitásszolgáltató és a tartalomszolgáltató között, azt jelenti, hogy a SP megbízhat az IdP-ben, hogy az hitelesítse a felhasználót, így mentesítve a SP-t a jelszavak és felhasználónevek tárolása alól. Ha az account adatai nem oszthatók meg akkor mind az IdP-nek mind az SP-nek külön kell accountokat kezelni a felhasználónak, így kényszerítve őt, hogy több account bejelentkezési adatait megjegyezze.
- A *tranzakció (üzleti tranzakciókkal kapcsolatos) attribútumok megosztása* igényli, hogy az IdP és SP megegyezzen a szerepekről, jogosultságokról vagy a felhasználó csoporthoz tartozásáról. Ezt nehéz megvalósítani, mivel két egymástól független szolgáltató jellemzően különböző megoldást alkalmaz az identitások csoportosítására illetve a szerepek információinak kezelésére. A tranzakciós attribútumok megosztása helyett, egy szolgáltató leképezheti a tranzakciós attribútumaikat, olyan alakban, amit az üzleti partnerük megért. Ebben a megközelítésben az azonosítási meta-adatot külön kezelik az IdP-nél és az SP-nél.
- A *profil attribútumok megosztása* az IdP és az SP között általában felhasználói beleegyezés kérdése. A felhasználó preferenciáitól és a bizalmassági igényeitől függ. Ezen attribútumok megosztásához szükség van felhasználói beleegyezésre illetve képesség ennek igazolására. Gyakorlati értelemben, bizonyos attribútumok megoszthatók (ilyen például az e-mail cím) míg más attribútumok nem. Ha nem megoszthatóak, akkor duplikálni kell őket az IdP-nél és az SP-nél is. Tehát, például ha egy felhasználó lakás címe duplikálva van, akkor külön kell kezelnie az üzleti partnereknek. Ha a felhasználó elköltözik és az egyik üzleti partner ismeri az új címet, a különálló azonosítási modellben, az üzleti partner nem tudja értesíteni erről az információról a többieket.

Különálló

A különálló megközelítés a szövetségi üzleti interakciókban akkor alkalmas, ha a két szervezet nem oszthat meg azonosítási információt. Ennek oka lehet adatok elkülönítése, közvetítés-ellenesség (verseny okok miatt a vállalatok nem szeretnék megosztani az ügyfél-információkat), politikai okok vagy, mert a felhasználónak mindkét szolgáltatóval van külön kapcsolata.



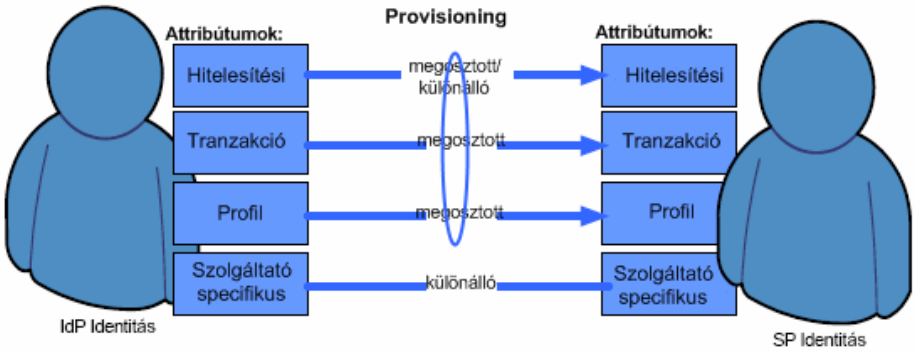
8. ábra: Különálló azonosítási modell

A különálló azonosítási adat menedzsment modellben, azonosítási adatok kezdetben egyeztethetők az üzleti partnerek között a kezdeti account beállítás részeként, habár később külön fogják kezelni őket.

Azonosítási attribútumok

A szövetségi modellben az IdP-nek és a SP-nek meg kell egyeznie a megosztható és a külön kezelt információról. Ezen információ – az identitást érintő - több típusú adatból áll:

- Bejelentkezési adatok
- Tranzakció attribútumok
- Profil attribútumok
- Szolgáltató-specifikus attribútumok



9. ábra: Megosztott és különálló azonosítási adatok és attribútumok

Az *azonosítási adatok* mindegyik típusánál, lehetséges *megosztott* vagy *különálló* azonosítási adat menedzsment (lásd: 9. ábra). Így mikor felmérik a szövetségi modell provisioning elvárásait, akkor kiértékelik a különböző típusú azonosítási adatok közül mindegyiknek a megosztott/különálló mivoltát.

Bejelentkezési adatok

A bejelentkezési adatok olyan információk melyeket egy identitás hitelesítésére használnak. Ez az információ egy felhasználó azonosítójához köthető (úgy, mint felhasználói név vagy azonosító). A bejelentkezési azonosítók adatként vannak ábrázolva, mint például a jelszó vagy a hardver „kulcsról" (token) generált egyedi PIN kód. Ezeket a hitelesítő adatokat egy felhasználó mutatja fel – a hitelesítési folyamat részeként – a saját identitásának bizonyítékaként. Ez azt foglalja magába, hogy egy felhasználó hitelesítéséhez, a szövetségi üzleti partnernek rendelkeznie kell egy másolattal a felhasználó bejelentkezési adatairól, vagy valamilyen más eszközzel a felhasználó bejelentkezési adatainak érvényesítésére. Így a jelenlegi hitelesítési modellek különálló azonosítási adatmodellt igényelnek (mindegyik üzleti partner rendelkezik egy másolattal az user bejelentkezési adataiból.)
Az egyik célja a szövetségi modellnek, hogy a megosztott azonosítási adatmodellre váltás. A bejelentkezési adatokra nézve ez azt jelenti, hogy egy szövetségi üzleti partnernek képesnek kell lennie arra, hogy bízzon egy harmadik félben (egy identitásszolgáltatóban), hogy az kiértékelje a felhasználó bejelentkezés-adatait és kijelentsen valamilyen biztonságos, megbízható információt, amit felhasználhatnak, hogy kezeskedjen a felhasználó - identitásszolgáltatónál történt - sikeres hitelesítéséért. Így a szövetségi modellben a bejelentkezési adatok kibővíthetők, hogy IdP-től származó biztonsági tokeneket tartalmazzanak, bizonyítva a felhasználó azonosságát. A megosztott modellre való váltás a bejelentkezési adatok számára azt jelenti, hogy a szövetségi üzleti partnerek viselkedhetnek tartalomszolgáltatóként és nem kell többé azonosítási adatokat kezelniük.
A szövetségi üzleti interakciók megosztott azonosítási megközelítése megfelelő lehet, amikor egy üzleti partner képes megbízni egy identitásszolgáltató által egy felhasználóról tett kijelentésben anélkül, hogy függetlenül attól jóváhagyta volna a felhasználó bejelentkezési adatait. Ebben a modellben a szövetség lehetővé teszi a felhasználónak (és a federációs üzleti partnereknek), hogy létrehozzanak egy közös egyedi azonosítót, amellyel utalhatnak a felhasználóra, ugyanakkor ez az azonosító semelyik üzleti partnernél sem tartalmaz információt a felhasználóról. Ez alapján a közös azonosító alapján az identitásszolgáltató képes arra, hogy szövetségi üzleti partnereknek bocsásson ki SSO információt.
A megosztott azonosítási modellben nincs szükség a bejelentkezési adatok karbantartására. Azonban szükséges létrehozni a két üzleti partnernél helyi identitást és közös azonosítót a

felhasználónak. Ezt provisioning megoldásokkal kezelik. Általában a különálló azonosítási modell nem tartalmaz provisioning megoldást. Az ilyen szövetségi modellben a felhasználónak külön accountja van az üzleti partnereknél. A különálló azonosítási adat menedzsment modellben, az azonosítási adatok kezdetben egyeztethetők az üzleti partnerek között a kezdeti account beállítás részeként, habár később külön fogják kezelni őket.

Tranzakció attribútumok

A tranzakció attribútumok információt tartalmaznak a felhasználóról, a csoporthoz tartozásáról és jogosultságairól. Ez az információ az user azonosítójához kötődik. Ez olyan csoportokat tartalmazhat, amikhez a felhasználó tartozik, vagy olyan szerepeket, melyeket felvehet. Ez az adat tartalmazhat további azonosítókat (úgy, mint ügyfél azonosító, törzs utas státusz, egészség biztosítási azonosító, hitelkártyaszám, stb.) speciális szervezeti szerepeket (például HR menedzser, tőzsdeügynök, középvezető, ellenőr, stb.). Ezeket az információkat gyakran használják a jogosultság/hozzáférés vezérlési döntések meghozatalának részeként tranzakció szinten (például egy bizonyos HR menedzser tudja-e frissíteni egy alkalmazott státuszát?). Ezeket az információkat javarészt nem a felhasználó kezeli. Általában egy felhasználó tranzakció attribútumai nem közösek az összes IdP és SP között.
A tranzakció attribútumok megosztásával, az egyik fél (általában az IdP), a felhasználóval kapcsolatos tranzakció attribútum információk *hiteles forrás*aként viselkedhet. Az attribútum információk naprakészen tartása az IdP és SP között prioritást élvező módon zajlik, tehát ha az IdP-nél frissül az információ, egy sürgős kérés (priori provisioning request) segítségével megpróbálják az SP-nél frissíteni az információt. Az attribútum információ kezelése, dinamikus, just-in-time módszerrel is lehetséges, ami azt jelenti, hogy a frissített/új információ a SSO válasz részeként érkezik az SP-hez vagy válaszként a SP-től származó direkt kérésre.
Ha a tranzakció attribútumokat külön kezelik a szövetségben, akkor mindegyik federációs üzleti partner felelős a naprakész attribútum kezelésért, tehát nincs provisioning megoldás. A különálló azonosítási adat menedzsment modellben, a tranzakció attribútumok kezdetben egyeztethetők az üzleti partnerek között a kezdeti account beállítás részeként, habár később külön fogják kezelni őket. Megjegyzendő, hogy mivel az attribútumokat nem a felhasználó kezeli ezért a naprakész menedzsment a SP adminisztrátoraira hárul.

Profil attribútumok

A profil attribútumok kiegészítő információt képviselnek, ami nem köthető közvetlenül a hitelesítési vagy jogosultság döntésekhez. A profil attribútumok információ specifikusak lehetnek a felhasználói identitás számára, ilyenek az e-mail cím, lakáscím, születési dátum és telefonszám. Az azonosítási profil attribútumok preferenciát vagy testre szabás attribútumokat tartalmaznak, mint például törzs utas azonosító, helyi információ és előfizetési információ (például, a felhasználó újság előfizetései, stb.). Ezt az információt a másodlagos felhasználói identitás érvényesítés részeként használhatják (elfelejtett jelszó visszaszerzési eljárás részeként), továbbá egy hozzáférés vezérlés döntés részeként használhatják olyan forgatókönyvekben, ahol hozzáférést a felhasználó kora vagy a lakhelye alapján korlátozzák. Ezt a felhasználóval kapcsolatos információt általában önmaga kezeli. A felhasználó profil attribútumok rendszerint megegyeznek az IdP-nél és a SP-nél. Ismerősebb környezetbe helyezve, nézzünk egy NagyCég alkalmazottat, Első urat, aki részt vesz egy tetszőleges légitársaság törzs utas programjában. Első úrnak online accountja van RBTravel-nél ahol előjegyzi a repüléseit, ez az account az identitáshoz kötődik. Ezzel a felhasználói névvel van összekapcsolva Első úr jelszava (bejelentkezési adatok) melyeket hitelesítésre használnak, ezeket Első úr nem ismeri mivel a provisioning részeként lettek beállítva NagyCégtől. Első úr utazási accountjával összekapcsolódnak a profil attribútumok (számlázási cím, telefonszám).
Első úr utazási accountja alapján, az utazási szolgáltató meghatározza (és kezeli) az ő törzs utas-státuszát (tranzakció attribútum). A repülőjegy előjegyzésnél Első úr attribútumait használják fel, hogy segíthessék őt a jegyrendelésnél, továbbá, hogy kibocsássák a törzs utas kártyájára a jegyet. Amikor Első úr előjegyez egy utazást, az utazási osztályt olyan attribútumok alapján dönthetik el, mint a légitársasági pontok vagy a NagyCégnél betöltött helye. Amikor Első úr kiválasztotta a kívánt utazást és előjegyezi azt, az identitásának másodlagos ellenőrzése végbemegy Első úr számlázási cím specifikációjának részeként (ahová a megrendelés jóváhagyásához szükséges információ fog érkezni).
A provisioning megoldásokkal az IdP létrehozhat, frissíthet felhasználói profil attribútum információkat (e-mail, személyes információ, lakcím, tagsági és előfizetői) és szolgáltatás-specifikus attribútumokat egy felhasználóról a SP-knél. Ezeket az attribútumokat általában a *végfelhasználó* kezeli a profil információk szerkesztésével az IdP-nél.

Szolgáltató-specifikus attribútumok

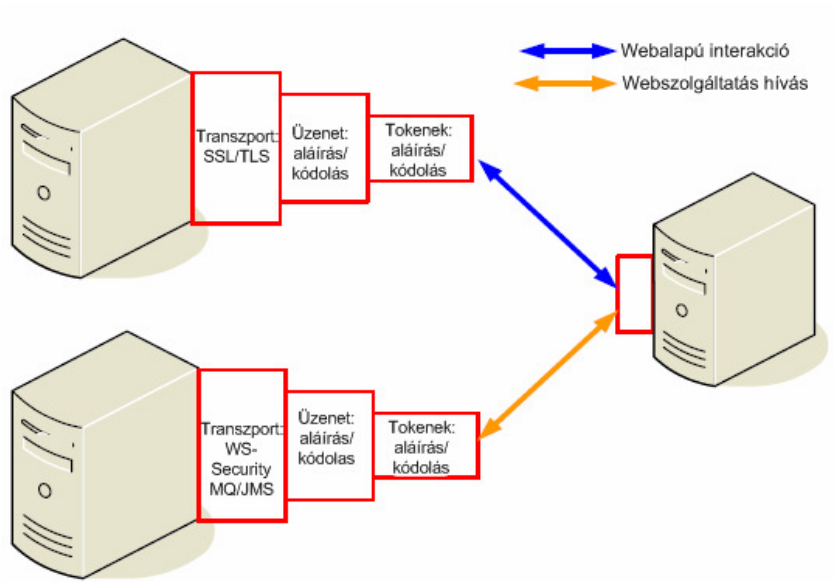
A szolgáltató-specifikus attribútumok tartalmazhatnak tranzakció és profil attribútumokat, melyek lényegesek egy adott felhasználó számára egy adott tartalomszolgáltatónál; ezek az információk nem megosztottak az SP-k között. Erre példa a felhasználó vásárolt áruinak listája egy aukciós portálon és a kedvezmények (ingyenes házhozszállítás) melyek ennek a felhasználónak a tranzakció előzményeihez kapcsolódnak. A szolgáltató-specifikus profil attribútumokra példa az user azon preferenciája, hogy mindig a „25$-nál olcsóbb játékok" kategóriában keresi az új árveréseket.

A felhasználó szolgáltató-specifikus attribútumai olyan attribútumok melyeket nem osztanak meg a szövetségi üzleti partnerek között és nem igényelnek provisioning megoldásokat.

Bizalom

A bizalom kulcsképesség mindhárom területen, ennek következtében kulcsfontosságú a szövetségi azonosítás menedzsmentben.

A bizalmi kapcsolat, technikai szinten a kriptográfiai kulcsok használatával jelenik meg. Ezek a kriptográfiai technikák biztosítják a bizalmi infrastruktúrát, melyre épülhetnek a szolgáltatások. A federációs üzleti partnereknek szükségük van a biztonságos és megbízható információcserére, hogy biztosítsák az elvárt felhasználói élményt. Ez a bizalmi infrastruktúra használatával vihető véghez.



10. ábra: A bizalom rétegei

A bizalmi infrastruktúra lehetővé teszi az üzenetek védelmét minden szinten:

Transzport	A felhasználó alapú szövetségi azonosítás menedzsment (FIM) kommunikációt SSL-lel védik, az applikáció alapú FIM kommunikációt pedig WS-Security-vel.
Üzenet	Aláírás és titkosítás segítségével nyújt bizalmasságot és integritás védelmet a FIM adatfolyamban lévő üzeneteknek.
Token	Biztonságos tokenek használatával közölhető információ egy felhasználóról a FIM adatfolyam bizonyos lépéseinek részeként.

A bizalmi infrastruktúra védelmet nyújt az érvénytelen vagy tisztességtelen FIM adatfolyamok ellen miközben lehető legnagyobb tekintettel van a bizalmi információ kezelésére.

Transzport

A legegyszerűbb formáját a bizalmi infrastruktúrának a transzport réteg SSL protokollja nyújtja, mellyel két üzleti partner között a transzport rétegen kódolható a kommunikáció. A vállalkozások általában tudják kezelni a SSL tanúsítványokat, és tudják, hogy miként használják azokat például kölcsönösen autentikált SSL-t használó vállalatok hitelesítésére. Az SSL alapú bizalmi infrastruktúráknak sajnos korlátai vannak például az, hogy (legfeljebb) pont-pont alapúak nem pedig végpont-végpont.
A Web szolgáltatások, azonban nem mindig futnak SSL-kompatibilis transzport protokoll felett; a Web szolgáltatásokat olyan transzport réteg protokollokon keresztül lehet hívni, mint a JMS[4] vagy MQ[5]. A Web szolgáltatások bizalmi infrastruktúrája nagyobb flexibilitást igényel, mint amit az SSL kínál. Ezt a rugalmasságot a Web szolgáltatás kérések aláírása és a titkosítása nyújtja, a tetszőleges transzport réteg-védelmen felül.
A szövetségi azonosítás menedzsment kérések általában http felett futnak (és így ki tudják használni az SSL előnyeit). Ezek azonban nem pont-pont kommunikációk, ami azt jelenti, hogy szükség van egy plusz védelmi rétegre. Ezt a FIM kérések aláírása és a titkosítása nyújtja, a tetszőleges transzport réteg-védelmen felül.

[4] A **Java Message Service** (röviden **JMS**) egy Java API, amellyel üzeneteket lehet küldeni különböző szoftverkomponensek között. - http://hu.wikipedia.org/wiki/Java_Message_Service
[5] A számítástechnikában a Message Queue-k (MQ) szoftverek-tervezési elemek, amiket processz-közi vagy szál-közi kommunikációra használnak ugyanazon a processzen belül. – az Wikipedia angol nyelvű cikke nyomán http://en.wikipedia.org/wiki/Message_queue

Üzenet

Mind a Web szolgáltatások mind a szövetségi azonosítás megoldások, egy nem transzport alapú bizalmi infrastruktúrát igényelnek. Ez az *üzenet* réteg kéréseinek aláírásával és titkosításával érhető el. A bizalmi szolgáltatás nyújtja az infrastruktúrát az aláíráshoz és titkosításhoz használt, kulcsok és tanúsítványok kezeléséhez.

A *bizalmi szolgáltatás* a szervezeti saját kulcsok és tanúsítványok kezelésének egy módját nyújtja és annak, hogy miként kössük az üzleti partner tanúsítványait (melyeket egy harmadik fél Tanúsító Hatóság (Certificate Authority) leellenőrzött) a saját, üzleti-megállapodással jóváhagyott, üzleti partner identitáshoz. Ezeket a kulcsokat aztán üzenetek aláírására/hitelesítésére és titkosítására/visszafejtésére használják az üzleti partnerek között, függetlenül minden transzport réteg biztonságtól.

Token

Ráadásként az üzenet réteg biztonságához, az üzenetek *tokeneket* tartalmazhatnak, hogy egy kérés küldőjéről, biztonság-specifikus információt továbbítsanak (például hitelesítési és/vagy autorizációs célokra). Ez az információ a bizalmi infrastruktúra részét képzi, ugyanúgy ahogy a kulcsok aláírás/titkosítás célokat szolgálnak: Rendeltetésszerű használat esetén a token, a felmutatójával kapcsolatos információt szállít.

A *bizalmi szolgáltatás* a biztonságos tokenek kezelésének egy módját nyújtja. A tokenek (legalább) egy üzleti partnerrel közösek és előre-egyeztetett, biztonságilag lényeges információt tartalmaznak. A tokenek aláírással és titkosítással védettek, gyakran ugyanazzal a titkosítással, mint amit az üzenet rétegnél használnak.

Szövetségi protokoll

Amikor szövetséget hoznak létre, a technikai szinten megállapodást kell kötni arról, hogy milyen FIM szabványt használnak a federációban. Az identitásszolgáltató és a tartalomszolgáltató is általában többfélét támogat, de mindegyik szövetségi kapcsolathoz definiálni kell egyet.

Szabványok és törekvések

Az egyszerűsített bejelentkezési technikákat és megoldásokat már évek óta alkalmazzák. A szövetségi azonosítás menedzsment gyökerei a bejelentkezési technológiában vannak. Az első szabványosítási törekvések az Internet (*Shibboleth*) és az OASIS (*SAML*) által

történtek. Azóta a szövetségi törekvéseket a Liberty Alliance vezette (*Liberty ID-FF*) majd később a SAML szabvány részévé vált. A következőkben a szövetségi azonosítás menedzsmenttel kapcsolatos szabványokat, mutatom be, a SAML-t, mint az egyik legalapvetőbb szabványt részleteiben is.

SSL/TSL

Az SSL (Secure Socket Layer) egy protokoll réteg, amely a szállítási rétegbeli protokoll (pl. TCP/IP) és valamely alkalmazási rétegbeli protokoll (pl. HTTP) között helyezkedik el, az OSI terminológia szerinti viszony- és megjelenítési réteg feladatait látva el. Web böngészésnél például az SSL biztosítja a biztonságos kommunikációt a kliens (böngésző) és a szerver (web szerver) között. Autentikációhoz digitálisan aláírt tanúsítványokat használ, a kommunikáció titkosítva zajlik (az SSL handshake során közösen megegyeznek egy kulcsban, ebből generálják azután az egy session erejéig használatos session key-t, és ezt használják valamely szimmetrikus titkosító algoritmussal, pl. DES, AES, stb.).

A Secure Socket Layer (SSL, és utódja a Transport Layer Security, TSL) titkosítás segítségével nyújt session-szintű biztonságot. Bár nem gyakran gondolnak rá, mint identitás menedzsment protokollra, az SSL használható a küldő és fogadó fél hitelesítésére digitális tanúsítványokon keresztül, adatintegritás ellenőrzésére és a bizalmasság biztosítására. Mint olyan, az SSL gyakran az első (és egyetlen) opció, amelyet figyelembe vesznek az Internetes tranzakciók biztosításakor. Használható mind böngésző-Web szerver és szerver-szerver közti kommunikációban.

A népszerűsége ellenére SSL-nek van néhány hiányossága a következő területekben:

Tagoltság Bármely a session fölötti adat, vagy egészét titkosítják vagy semennyit sem. Ez csökkentheti a teljesítményt abban az esetben mikor nagy mennyiségű adatot kell cserélni, de kisméretű csomagokat kell csak titkosítani/visszafejteni ezen belül.

Végponttól-végpontig A SSL védelem véget ér, ha közbenső összetevőknek kell tranzakciókat megvizsgálniuk.

Security Assertion Markup Language (SAML)

Egy XML-alapú szabvány mely autentikációs (hitelesítési) és autorizációs (engedélyezés) adatok cseréjét teszi lehetővé biztonságos web domain-ok, tehát az *identitásszolgáltató* IdP

(tanúsítvány kiadója) és egy *tartalomszolgáltató* SP (tanúsítvány „fogyasztója") között. A SAML az OASIS Biztonsági Szolgáltatások Szakmai Bizottságának terméke. Az elsődleges és legfontosabb probléma, amit a SAML kezelni próbál a *Web-böngésző Single Sign-On* (SSO) problémája.

Single sign-on (SSO) – Webes egyszeri bejelentkezési módszer, amely olyan speciális formája a szoftveres azonosításnak, ami lehetővé teszi a felhasználó számára, hogy egy adott rendszerbe való belépéskor mindössze csak egyszer azonosítsa magát és ezután a rendszer minden erőforrásához és szolgáltatásához további autentikáció nélkül hozzáfér.
A Single sign-on megoldások bőségesek az intranet szintjén (cookie-k használata például) de ezen lehetőségek kibővítése az intraneten túlra problémás volt és a nem teljesen-együttműködő saját technológiák elburjánzásához vezetett. A SAML vált a döntő szabvánnyá, alapjául szolgálva sok Single Sign-On megoldásnak a vállalati azonosítás menedzsment problémakörben.
A SAML feltételezi, hogy a hivatkozott felhasználó (principal) bejegyzett legalább egy azonosítás szolgáltatóhoz. Ez az azonosítás szolgáltató vélhetően a hivatkozott felhasználó helyi hitelesítési szolgáltatásait látja el. Azonban a SAML nem írja le ezeknek a helyi szolgáltatásoknak az implementációit; csakugyan, a SAML nem törődik azzal, hogy a helyi azonosítási szolgáltatások miként vannak implementálva (azonban az egyes szolgáltatók minden bizonnyal igen).

Így tehát az tartalomszolgáltató az azonosítás szolgáltatójára támaszkodik a hivatkozott felhasználó azonosítása érdekében. A hivatkozott felhasználó kérésénél az azonosítás szolgáltató SAML assertion-t küld az tartalomszolgáltatóhoz. Az assertion alapján, az tartalomszolgáltató egy hozzáférés vezérlési döntést hoz.

A SAML története

Az OASIS Biztonsági Szolgáltatások Szakmai Bizottságát (SSTC), amely 2001 januárjában ült először össze, kérték fel, hogy "definiáljanak egy XML keretrendszert az autentikációs és autorizációs információk cseréjére." [1] Végül a következő szellemi tulajdon létrejöttéhez járult hozzá az SSTC ezen év első két hónapjában:

- *Security Services Markup Language* (S2ML) a Netegrity-től
- *AuthXML* a Securant-tól

- *XML Trust Assertion Service Specification* (X-TASS) a VeriSign-től
- *Information Technology Markup Language* (ITML) a Jamcracker jóvoltából.

Ezen projekt munkálatai közben 2002 novemberében az OASIS kihirdette a Security Assertion Markup Language (SAML) V1.0 specifikációt, mint OASIS szabványt.

Eközben a Liberty Alliance, cégek, non-profit és kormányzati szervezetek egy nagy konzorciuma, tervezett egy kiegészítést a SAML szabványhoz melyet Liberty Identity Federation Framework (ID-FF, Szabadság Azonosítási Federációs Keretrendszer). Mint elődjét, a Liberty ID-FF-t is egy szabványosított domain-közti, web-alapú, SSO (egyszeri bejelentkezés) keretrendszernek tervezték. Ráadásként, a Liberty meghatározta a *bizalom körét*, ahol mindegyik résztvevő domain megbízható és pontosan dokumentálja az eljárást, amellyel a felhasználót azonosítják, az alkalmazott autentikációs rendszer típusát, és bármely elvet, amely kapcsolatos az eredményező autentikációs bizonyítványokkal. A bizalom körének többi tagja megvizsgálhatja ezen elveket, hogy eldöntsék megbíznak-e az információkban.

Miközben a Liberty az ID-FF-et fejlesztette, az SSTC a SAML szabvány elsődleges javításán kezdett dolgozni. Ennek eredményeként jött létre a SAML V1.1 specifikáció, melyet a SSTC 2003 szeptemberében hagyott jóvá és melyet széles körben implementálnak és alkalmaznak ma is. Szintén ebben a hónapban Liberty az ID-FF-t az OASIS-nek adta - ezáltal elültetve a következő fő SAML változat magjait. Így 2005 márciusában, kihirdették a SAML V2.0-t, mint OASIS szabványt. A SAML V2.0 reprezentálja a Liberty ID-FF és egyéb szabadalmazott kiegészítések egyesülését, beleértve a SAML korábbi változatait is.

A SAML építő elemei

A SAML jó néhány létező szabványra épül:

Extensible Markup Language (XML)

> A legtöbb SAML elem az XML egy szabványosított dialektusában íródott, amely a SAML nevének alapját is adta (Security Assertion Markup Language).

XML Séma

> SAML assertion-ök és protokollok (részben) XML Sémában lettek specifikálva.

XML Szignatúra

Mind a SAML 1.1 és a SAML 2.0 digitális aláírást használ (az XML Szignatúra szabványon alapulva) az autentikációra és az üzenetek integritásának megőrzésére.

XML Kódolás

XML kódolás használatával, a SAML 2.0 elemeket szolgáltat a kódolt névazonosítók, kódolt attribútumok, és kódolt assertion-ök használatára (a SAML 1.1-nek nincsenek kódolási lehetőségei).

Hipertext Transzfer Protocol (HTTP)

A SAML erősen támaszkodik a HTTP-re, mint kommunikációs protokollra.

SOAP

SAML részletezi a SOAP használatát, különösen a SOAP 1.1-t.

A SAML anatómiája

A SAML XML-alapú assertion-öket, protokollokat, binding-okat (kötések) és profilokat definiál. A *SAML Core (mag)* kifejezés SAML assertion-ök általános szintaktikájára és szemantikájára utal, továbbá a protokollra, amelyen küldhetőek és fogadhatóak ezen assertion-ök egyik entitástól a másikig. A *SAML protokollok* arra utalnak, **amit** továbbítunk, nem pedig **ahogyan** (az utóbbit a binding típusa határozza meg). Tehát SAML Core "csupasz" SAML assertion-öket definiál SAML kérés és válasz elemekkel együtt.

A SAML binding határozza meg, hogy a SAML kérések és válaszok miként képezhetők le, egyszerű üzentekre illetve kommunikációs protokollokra. Egy fontos (szinkron) binding a SAML SOAP binding.

A SAML profil a konkrét megnyilvánulása egy jól definiált használati esetnek mely assertion-ök, protokollok és bindingok bizonyos kombinációját használja.

SAML assertion

A SAML assertion egy olyan adatcsomag, ami nulla vagy több, hiteles fél által kimondott állítást, „igazolást” hordoz.

<saml:Assertion ...**>**

...

</saml:Assertion>

Lényegében, egy résztvevő fél a következő módon értelmezi az assertion-t:

Az *A* Assertion *t* időpontban lett kibocsátva *R* által arra vonatkozólag, hogy *S* alany által szolgáltatott állítások (*C)* érvényesek.

SAML assertion-ök általában az azonosítás szolgáltatóktól az tartalomszolgáltatókhoz továbbítódnak. Az assertion-ök *állításokat* tartalmaznak melyek alapján az tartalomszolgáltatók hozzáférés-vezérlési döntéseket hoznak.

Ilyen állítás lehet:

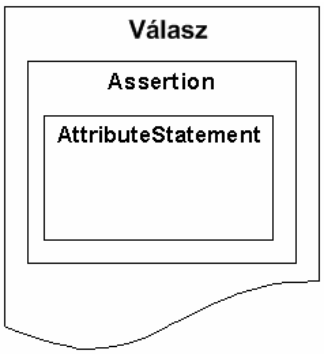
- Authentication Statement (Hitelesítési kijelentés) - pl. „Anna a publikus kulcsával azonosította magát, 2008. május 3-án délután 14 óra 30 perckor."
- Attribute Statement (Attribútum kijelentés) - pl. „Anna menedzser, és a budapesti kirendeltségen dolgozik."
- Authorization Decision Statement (Autorizációs döntés) - pl. „Anna hozzáférhet a budapesti CRM rendszer adataihoz." (a SAML2-ben elavultnak jelölik az autorizáció ilyen megoldását, és az XACML (eXtensible Access Control Markup Language) szabványt javasolják helyette)

Authentication statement-ek kijelentik az tartalomszolgáltatóknak, hogy az ügyfél valóban hitelesítette magát egy azonosítás szolgáltatóval egy adott időpontban egy adott hitelesítési eljárással. (Az AuthnStatement tartalmazza az alany hitelesítésének igazolását.) Egyéb információknak a hitelesített ügyfélről (az ún. *authentication context*) authentication statement-ben benne kell lenniük.

Az *attribute statement* kijelenti, hogy az alany összefüggésben van bizonyos attribútumokkal. Egy *attribútum* egy egyszerű név-érték pár. A résztvevő fél az attribútumokat a hozzáférés-vezérlési döntések meghozásához használja.

Az *authorization decision statement* kijelenti, hogy az alany végrehajthat *A* tevékenységet az *R* erőforráson *E* bizonyítás szerint. Az autorizációs döntés kijelentések szemléletessége a SAML-ban szándékosan korlátozott. Az összetettebb használati esetekben az XACML használata javasolt helyette.

SAML protokollok



11. ábra: SAML protokoll

A SAML *protokoll* írja le, hogy az egyes SAML elemeket (beleértve az assertion-öket) miként képezhetjük le SAML kérés és válasz elemekre, továbbá azon feldolgozási szabályokat, melyeket a SAML entitásoknak be kell tartaniuk mikor felhasználják vagy létrehozzák ezen elemeket. A legtöbb esetben, a SAML protokoll egy egyszerű kérés-válasz protokoll.

A SAML protokollüzenetek a következő problémákat oldják meg:

- Egy vagy több assertion visszaadása.
- Hitelesítés kérése és erre válasz küldése a hitelesítés tényét igazoló assertion-ként.
- Account-összekapcsolási azonosító („name identifier”) bejegyzése, megszüntetése és lekérdezése.
- Protokollüzenet megszerzése egyedi azonosító („artifact”) alapján.
- Összekapcsolódott munkamenetek közel egyidejű megszüntetése („single log-out”)

A legfontosabb típusa a SAML protokollkérésnek az ún. *query*. Az tartalomszolgáltató küld egy query-t az azonosítás szolgáltatónak egy biztonságos csatornán keresztül. Így a query üzenetek tipikusan SOAP-hoz kapcsolódnak.

Hasonlóan a statement-ekhez, a SAML query-knek is három típusa van:

1. **Authentication query**
2. **Attribute query**
3. **Authorization decision query**

Ezek közül talán az *attribute query* a legfontosabb (és alanya sok kutatásnak). Az *attribute query* eredménye egy SAML válasz mely egy assertion-t tartalmaz, mely maga is tartalmaz egy attribute statement-et.

SAML 1.1 protokollok

A query-ken túl a SAML 1.1 nem specifikál más protokollt.

SAML 2.0 protokollok

A SAML 2.0 meglehetősen kibővíti a *protokoll* fogalmát. A következő protokollok a SAML 2.0 magban vannak részletesen leírva:

- Assertion Query és Request protokollok

  Ezen protokollok már létező munkamenet esetén használhatóak további információk elkérésére. Segítségükkel az tartalomszolgáltató attribútumokat, hozzáférés vezérlési döntéseket kérhet a megfelelő entitástól (szervtől).

- Authentication Request protokoll

  Amikor egy felhasználó egy munkamenetben először látogat meg egy tartalomszolgáltatót, fel kell mutatnia egy olyan assertion-t, amely egy azonosítás szolgáltatónál történt sikeres hitelesítését igazolja (Authentication statement). Ezen assertion-t az tartalomszolgáltató egy Authentication Request protokollüzenet segítségével kéri el az azonosítás szolgáltatótól. A hitelesítési kérés eredményeképp az azonosítás szolgáltató vagy (újra) hitelesíti a felhasználót, vagy a már létező munkamenet esetén kiállítja a hitelesítést igazoló assertion-t.

- Artifact Resolution protokoll

  Az Artifact Resolution protokoll egy olyan mechanizmust definiál, aminek segítségével a SAML assertion-ök referencia szerint kerülnek átvitelre két rendszerentitás között, majd az assertion címzettje szinkron transzport protokollon keresztül a referencia segítségével elkéri a konkrét assertion-t a kiállító féltől. Ez a

szinkron transzport protokoll a gyakorlatban általában a SOAP (Simple Object Access Protocol), ami az XML web szolgáltatások transzport protokollja.

Az artifact tulajdonképpen egy kisméretű adat, ami azonosítja az assertion küldőjét, és magát az assertion-t. Ez a kisméretű adat a legegyszerűbb bindingok (például HTTP/GET) segítségével is átadható, és kevésbé érzékeny a hiteles és megbízható üzenettovábbításra. Az assertion ezután egy védett csatornán kerülhet átvitelre közvetlenül a szolgáltatók között, így a plusz indirekcióból akadó problémák mellett több előnye is van ezen megoldásnak.

- Name Identifier management protokoll

  Miután az azonosítás szolgáltató hozzárendelt egy azonosítót a felhasználóhoz (a konkrét tartalomszolgáltató munkamenetet figyelembe véve), ezen azonosító formátumát és tartalmát a ManageNameIDRequest üzenet segítségével változtathatja meg. Szintén ezt az üzenetet használja az azonosítás szolgáltató annak jelzésére, hogy az azonosító többé már nem használható. Természetesen egy ilyen változás végigterjedése a rendszerben némi időbe telik, ezért egy ideig még a régi azonosítóra történő hivatkozásokat is elfogadják az azonosítás szolgáltatók.

- Single Log out protokoll

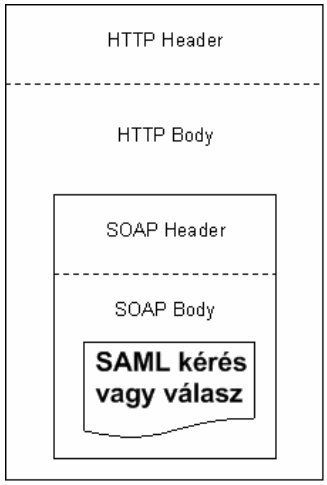
  Egyszeres kijelentkezésről beszélünk, amikor a felhasználót egy adott munkamenetbe csatlakozó összes tartalomszolgáltatónál közel azonos időben kijelentkezteti a munkamenetért felelős szerv (session authority). Ez akkor történik meg, amikor a felhasználó kijelentkezik bármelyik tartalomszolgáltatónál vagy közvetlenül a munkamenetet tároló szolgáltatónál - esetleg lejárt egy időkorlát, ami a rendszerben töltött időt szabályozza.

- Name Identifier leképezési protokoll

  Amennyiben egy tartalomszolgáltató és egy azonosítás szolgáltató közösen létrehoz egy azonosítót egy felhasználónak, az tartalomszolgáltató ezen azonosító alapján kérhet egy másik, speciálisabb formátumú azonosítót ugyanehhez a felhasználóhoz. Ezen használati esetet valósítja meg a Name Identifier leképezési protokoll két üzenete.

A legtöbb protokoll ezek közül teljesen új a SAML 2.0-ban.

SAML bindingok



12. ábra: SAML binding

A termékek közötti teljes együttműködéshez az kell, hogy a protokollüzenetek konkrét szállítási, üzenettovábbítási protokollokra való leképzése is szabványos legyen. Ezt a leképzést írja le a SAML bindingok specifikáció. Egy konkrét binding alatt a specifikáció általában a teljes kérés-válasz üzenetváltás átvitelét érti. A SAML protokollok: üzenetek és kommunikációs minták leképzése konkrét szállítási protokollra (HTTP, SOAP). Például, a SAML SOAP binding leírja, hogy a SAML üzenetet miként zárjuk a SOAP „borítékba", melyet magát egy HTTP üzenethez kötünk.

SAML 1.1 bindingok

A SAML 1.1 egy binding-ot specifikál, a SAML SOAP Binding-ot. Ráadás a SOAP-hoz, a SAML 1.1-ben implicit Web Böngésző SSO mely az előfutára a HTTP POST Binding-nak, a HTTP Redirect Binding-nak és a HTTP Artifact Binding-nak. Ezeket explicit nem definiálják, és csak a SAML 1.1 Web Böngésző SSO-val kapcsolatban használják. A binding fogalma nincs teljesen kifejlesztve egészen a SAML 2.0-ig.

SAML 2.0 bindingok

A SAML 2.0 teljesen elválasztja a binding fogalmat az alapul szolgáló profiloktól. Sőt a SAML 2.0-ban teljesen új binding specifikáció van mely a következő önálló binding-okat definiálja:

- SAML SOAP Binding (alapja a SOAP 1.1)

  A SOAP egyszerűnek és általánosnak szánt, strukturált információk cseréjére kidolgozott elosztott kommunikációs protokoll. Üzenetformátuma XML alapú, és egyszerűen kiterjeszthető bármilyen konkrét szállítási protokollra, a meglevő rendszerek nagy többségénél azonban a HTTP feletti implementációja terjedt el (SOAP over HTTP). Ez a technológia az XML alapú web szolgáltatások világának alapja.

- HTTP Redirect (GET) Binding

  A SAML HTTP- Redirect binding segítségével a SAML protokollüzenetek HTTP URL paraméterekbe képezhetőek le, és vihetők át HTTP Get kérés segítségével. Mivel a konkrét HTTP kliens/szerver implementációk esetén az URL hossza limitált lehet, ezért ez a módszer csak rövid üzenetek átvitelére alkalmas megbízhatóan. Általános használati esete, amikor a SAML kérést kiállító rendszerentitás (SAML requester) és a kérés címzettje (SAML responder) kommunikációját a végfelhasználó web böngészőjén keresztül kell megoldani (SAML intermediary).

- HTTP POST Binding

  A HTTP- Post binding viselkedése és tulajdonságai erősen hasonlítanak a HTTP-Redirect binding-hoz. A fő különbséget az jelenti, hogy a SAML protokoll üzenetet ebben az esetben egy HTML FORM tartalmazza, amit a böngésző HTTP POST kéréssel küld el a SAML címzettnek. A HTTP-Redirect binding-hoz képesti előnye ennek a megoldásnak, hogy a szállított üzenet méretkorlátja feloldódik (web szervertől függően több megabájt a POST adat mérete, ami több mint elég egy SAML üzenetnek).

- HTTP Artifact Binding

  A SAML protokollüzeneteknél már előkerült az artifact fogalma. A HTTP Artifact binding pontosan erre a fogalomra (és a hozzá kapcsolódó ArtifactResolve protokollüzenetre) épít. Az artifact tulajdonképpen egy SAML üzenetre mutató „pointer”, aminek segítségével az eredeti üzenet elérhető.

- SAML URI Binding

- Reverse SOAP (PAOS) Binding

Ez az újjászervezés rendkívüli rugalmasságot eredményezett: vegyük csak példának a Web Böngésző SSO-t egyedül, az tartalomszolgáltató választhat négy binding közül (HTTP Redirect, HTTP POST és kétféle HTTP Artifact), míg az azonosítás szolgáltatónak három binding lehetősége van (HTTP POST plusz két formája a HTTP Artifact-nak), az összes (tizenkettő) elképzelhető lehetőség a SAML 2.0 Web Böngésző SSO Profilok közül.

SAML profilok

A SAMLv2 Profilok specifikáció az az összekötő kapocs, ami a SAML rendszerek együttműködését a legmagasabb szinten szabályozza. Minden SAML profil egy jól meghatározott használati esetet ír le, a használati eset megvalósításához szükséges pontos lépésekkel, a használt protokollok és bindingok megválasztásával és az alsóbb szintű építőelemek által nem tisztázott részletek megadásával. Ezek közül a legfontosabb a Web Böngésző SSO Profil.

SAML 1.1 profilok

A SAML 1.1 két profilt specifikál, a Böngésző/Artifact Profilt és a Böngésző/POST Profil-t. Az utóbbi az assertion-öket *érték alapján* továbbítja, amíg Böngésző/Artifact *referencia alapján*. Ennek következményeként a Böngésző/Artifact-nak egy védett kommunikációs csatornára van szüksége SAML SOAP feletti adat cseréhez.

A SAML 1.1-ben, az egyszerűség kedvéért minden adatfolyam egy azonosítás szolgáltatóhoz érkező kéréssel kezdődik. A szabadalmazott kiegészítések az alap IdP (azonosítás szolgáltató) által kezdeményezett adatfolyamokat tűzték ki célul. (pl.: Shibboleth).

SAML 2.0 profilok

A Web Böngésző SSO Profil-t teljesen átdolgozták a SAML 2.0-ban. Fogalmilag SAML 1.1 Böngésző/Artifact és Böngésző/POST speciális esetei a SAML 2.0 Web Böngésző SSO-nak. Az utóbbi jelentősen rugalmasabb, mint a SAML 1.1-beli megfelelője köszönhetően a V2.0 új "plug-and-play" binding konstrukciójának.

Ellentétben az előző változatokkal a SAML 2.0 böngésző adatfolyam az tartalomszolgáltatóhoz beérkező kéréssel kezdődik. Ez nagyobb rugalmasságot

eredményezett, de SP (tartalomszolgáltató) által kezdeményezett adatfolyamoknál felmerült az ún. *Identity Provider Discovery* probléma, amely ma is sok kutatás középpontjában áll.

A Web Böngésző SSO-n felül a SAML 2.0 számos új profilt tartalmaz:

- SSO Profilok
    - Web Browser SSO Profil
    - Enhanced Client or Proxy (ECP) Profil
    - Identity Provider Discovery Profil
    - Single Log out Profil
    - Name Identifier Management Profil
- Artifact Resolution Profil

  A HTTP- Artifact binding által használt mód a SAML protokollüzenetek elérésére azonosító alapján.
- Assertion Query/Request Profil

  Különböző típusú Assertion-ök lekérdezése, például Attribútum-átvitel vagy hozzáférés-vezérlés esetére.
- Name Identifier Mapping Profil

  Létező felhasználói azonosító cseréje egy adott munkamenet esetén.
- SAML Attribute Profilok

  A felhasználói profil attribútumainak pontos leképzését szabályozza különböző források (például LDAP) esetén.

SAML biztonság

Mivel a SAML assertion-ök sok esetben tartalmaznak üzenethitelesítést és integritást garantáló XML digitális aláírást illetve alkalmazható az üzenetben elemszintű titkosítás is, ezért nem minden esetben kell a szállítási protokollban biztosítani ezeket a kritériumokat. Általános irányelv, hogy amennyiben harmadik fél is része a kommunikációnak (például a felhasználó böngészője a SAML HTTP- Post binding-nál), akkor az üzenetszintű védelem az alkalmazandó megoldás. Ha két rendszerentitás közvetlen kapcsolatban cserél

információt (SAML SOAP binding), általában a transzport protokoll által nyújtott biztonság elegendőnek bizonyul.

Shibboleth

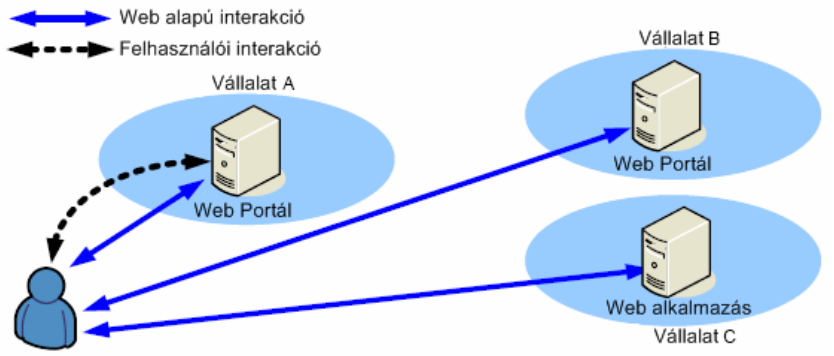
A Shibboleth rokonságban áll SAML-el de felső oktatási szektor számára készült. A SAML protokollok közül néhányat használ, de további sajátosságokat is tartalmaz. Itt mutatkozik be a WAYF feldolgozás elképzelése, mellyel a tartalomszolgáltató implementálhatja mind a push mind a pull alapú SSO protokollokat. A Shibboleth-et a SAML 2.0 specifikáció társaként mutatták be. Például, a felső oktatási közösségben nagyon szigorú szabályok vannak egy intézmény diákjaival kapcsolatos információ kibocsátásáról egy másik felső oktatási intézménynek.

WS-Federation

A WS-Federation egy szövetségi azonosítás specifikáció, amelyet a BEA Systems, BMC Software, CA Inc., IBM, Layer 7 Technologies, Microsoft, Novell, Ping Identity, és a VeriSign fejlesztett ki. A Web Services Security (Web szolgáltatások Biztonsága) keretrendszer részeként, a WS-Federation olyan technikákat határoz meg, mellyel eltérő biztonsági tartományok közvetíthetnek információt identitásokról, identitás attribútumokról és autentikációról.

Föderációs Single Sign-On

A szövetségi SSO (F-SSO) az eljárás, ami által egy felhasználó hitelesíti magát egy szövetségi üzleti partnernél (identitásszolgáltató, IdP) és az IdP kibocsát egy hozzá tartozó identitást (és attribútumait) az egyik/az összes szükséges (és megbízható üzleti partner) tartalomszolgáltatónak, a felhasználó online szövetségi tapasztalatainak részeként. A globális bejelentkezést a szövetségi single sign-on protokoll nyújtja. Ezek a protokollok biztosítanak szabványos, együttműködésre képes eszközöket a szövetségi üzleti partnereknek, hogy megegyezzenek a felhasználók bejelentkezési azonosítóinak prezentációjáról, az identitásszolgáltatótól a (megbízható) szövetségi tartalomszolgáltatóig.
A következőkben a szövetségi egyszeri bejelentkezést tanulmányozom részletesen.



13. ábra: Biztonságos felhasználói interakció – F-SSO

A 13. ábrán a felhasználói interakció egy egyszerűsített ábrázolása látható, ahol a felhasználó kommunikál az A jelű vállalattal, aki IdP-ként viselkedik, a két másik vállalat (B és C) SP-k. A kommunikáció Web böngésző alapú és F-SSO-t használnak az egyszeri bejelentkezésre. Az egyszerűsített bejelentkezés bármelyik SSO protokollal megoldható, SAML, Liberty ID-FF vagy WS-Federation.

Annak érdekében, hogy a F-SSO funkcióit bemutassam, a vállalati példánk környezetében vizsgálom őket.

A F-SSO szempontjából lényeges funkciók: pull és push SSO protokollok, account összekapcsolás, WAYF, sessionkezelés, kijelentkezés, bejelentkezési adatok eltakarítása, globális good-bye és account szétkapcsolás.

Push és Pull SSO

Az SSO-nak két módja van, push és pull. A pull SSO a SAML 1.x és 2.0-ban, a Liberty-ben és a WS-Federation-ben elérhető, a push a SAML 1.x-ben és a WS-Federation-ben. A push SSO azt jelenti, hogy a SSO adatcserét egy az IdP-hez érkező kérés indítja, amely küld (PUSH) egy biztonsági tokent a SP-nek. A pull SSO esetén a SSO adatcserét az SP-hez érkező kérés indítja, amely kér (PULL) egy biztonsági tokent az IdP-től. A NagyCég pull SSO-t használ, amikor az alkalmazottai bejelentkeznek RBTravel-hez.

Account összekapcsolás

Az eddigiekben csak az egyszeri bejelentkezésről volt szó - nem esett szó arról az SP oldalon felmerül problémáról, hogy plusz adatokat kell tárolni a felhasználóról (ami csak az adott alkalmazásra vonatkozik). Tovább bonyolítja a helyzetet, hogy a felhasználó személyiségi jogait is meg kell védeni a rendszerben, illetve probléma esetén az IdP oldalon

visszakövethető kell, legyen, hogy egy adott pillanatban melyik felhasználó melyik szolgáltatást vette igénybe. Az első felmerülő lehetőség, hogy az IdP oldalon tároljuk az összes információt. Ez nyilvánvalóan nem megtehető, több okból sem. Egyrészt felesleges terhelést és adminisztrációt jelent, ráadásul az IdP szempontjából lényegtelen információkról van szó. Másrészt, ilyenkor biztosítani kellene, hogy a többi SP ne jusson hozzá ezekhez az információkhoz. Sok esetben nem kerülhető ki tehát, hogy az SP is tároljon felhasználói adatokat, a felhasználó rendelkezzen lokális „account”-tal. Ez szinte minden esetben felmerül, hiszen például már egy egyszerű webes közösségi alkalmazás esetén sem megkerülhető hogy néhány attribútumot (legalább a becenév) megjelenítsen a felhasználókról. Valahogy össze kell tehát kapcsolni az IdP által adott felhasználói identitást az SP oldali adatokkal. Erre a következő megoldások merülnek fel:

Összekapcsolás az IdP által tárolt attribútumok alapján - ez a megoldás az egyszerűbb esetekben használható, de rengeteg problémát hordoz magában. Nem kezeli az esetleges attribútum változásokat (esetleg az attribútum-kiadási elvek változásait), és túl szoros csatolást visz a rendszerbe.

- *Összekapcsolás fix azonosító alapján* - az IdP minden felhasználóról nyilván tart egy fix azonosítót, amit a felhasználó nem változtathat, és ezt az azonosítót elküldi minden egyes SP-nek, aki éppen be akar kapcsolódni a felhasználó munkamenetébe. Tipikusan ez a fix azonosító lehet a felhasználó e-mail címe, vagy a tanúsítványán szereplő név. Sajnos ez a megoldás sem védi meg a felhasználó személyiségi jogait, hiszen két SP a felhasználó tudta és beleegyezése nélkül képes a saját lokálisan tárolt adataikat egyeztetni, ezzel egy nagyobb képet kialakítani a felhasználó tevékenységéről.
- *Összekapcsolás fix, de alkalmazásonként változó pszeudonim azonosító alapján* - a pszeudonimitás egy „álnevet” visz a rendszerbe, ami konkrét megvalósításban egy véletlenül sorsolt azonosító. Ráadásul minden SP más álnevet lát, de a többszöri látogatás során mindig ugyanazt. Ez a megoldás nem teszi lehetővé a személyes adatok előző pontban végiggondolt kiszivárgását. Az IdP felelőssége, hogy alkalmazásonként különböző véletlen álneveket adjon ugyanannak a felhasználónak, és gondoskodjon arról, hogy ezek az azonosítók perzisztensek maradjanak. Ez többlet adminisztrációval jár, ami miatt néhány IdP szoftver nem támogatja ezt a megoldást.

- *Összekapcsolás változó pszeudonim azonosító alapján* - ebben a megoldásban az IdP munkamenetenként más és más véletlen azonosítót rendel a felhasználóhoz, ami függ az SP-től is. Sajnos így elveszik az account összekapcsolás lehetősége, de probléma esetén a visszakövethetőség megmarad (általában egy beállítható, fix ideig meg kell őrződjenek a pszeudonimeket tároló naplófájlok, amiből rekonstruálható a felhasználó útja a rendszerben).

Ezeket az összekapcsolásokat alapvetően többféleképp is megtehetjük. Attribútum alapú összekapcsolásnál az SP az attribútumok alapján kikeresheti a megfelelő lokális felhasználói profilt és elvégezheti automatikusan az összekapcsolásukat. Egyébként a felhasználónak explicit módon be kell jelentkeznie mindkét rendszerbe, és ezzel az egyidejű bejelentkezéssel kötheti össze a kétféle azonosítóját (utóbbi megoldást általában a perzisztens pszeudonimek esetén szokás használni). Ez a felhasználó által kezdeményezett összekapcsolás más szempontból is előnyös: magára a végfelhasználóra bízza a döntést, így az adatkezelést is teljesen tisztává teszi. A legtöbb ilyen módon összekötött rendszer lehetővé teszi az összekapcsolt, „federált" azonosítók szétkapcsolását is. Automatikus összekapcsolás esetén az SP akár dinamikusan is létrehozhatja a lokális accountot, az IdP által adott attribútumok figyelembe vételével.
A fentieken kívül lehetőség van természetesen arra is, hogy a perzisztens azonosítók alkalmazásával automatikusan, előre összekössünk néhány konkrét SP accountot a hozzájuk tartozó identitással. Ezt „bulk federation"-nek hívják, és az üzleti rendszereknél gyakran alkalmazott megoldás.

Vegyük RBTelkom-ot és RBBanking-et ahol Kiss Józsefnek külön (hitelesíthető) accountja van mindkét vállalatnál. Amikor a két vállalat megegyezik a federációba csatlakozásról, akkor nekik valamilyen módon lehetővé kell tenni, hogy RBTelkom felhasználói SSO-val beléphessenek RBBanking-hoz. Ennek a megoldása RBBanking feladata. Ez két lépésben történik, jelen esetben RBTelkom weboldaláról indulva. RBTelkom megváltoztatja a hivatkozást a portálján, így az egyszerű átirányítás helyett, a bank linkjére kattintás egy SSO kérést indít RBBanking-hoz. A pénzintézet megkapja a kérést, de nem tudja megfeleltetni egy helyi identitásnak. Ez azt eredményezi, hogy RBBanking-nak el kell kérnie a bejelentkezési adatait Kiss úrtól. Sikeres hitelesítés esetén, RBBanking-nál hozzárendelődik a RBTelkom által kibocsátott CUID-hez (az SSO kérésből) a saját helyi felhasználó reprezentáció (József

direkt bejelentkezéséből). RBBanking most már képes account összekapcsolást létesíteni, így Kiss úr SSO-val bejelentkezhet RBTelkom-tól.

Ha a felhasználó a roll-over[6] időszakban akarja közvetlenül elérni RBBanking-ot, akkor őt a szokásos módon hitelesítik. Ezután, RBBanking SSO-t fog kérni RBTelkom-tól (a már hitelesített felhasználónak). A megfelelő SSO válasz tartalmazni fogja a közös felhasználói azonosítót (CUID), így RBBanking mind a RBTelkom által kibocsátott CUID-vel (az SSO kérésből) mind a saját helyi felhasználó reprezentációval (József direkt bejelentkezéséből) rendelkezni fog. RBBanking most már képes account összekapcsolást létesíteni, így Kiss úr SSO-val bejelentkezhet RBTelkom-tól.

RBBanking kikapcsolhatja a felhasználó helyi jelszavának kérését, így a közvetlen hitelesítés RBBanking-nál már nem lehetséges, addig ameddig a felhasználó accountja össze van kapcsolva RBTelkom-mal. Legközelebb, amikor a felhasználó megpróbál közvetlenül hozzáférni RBBanking-hez, a bank SSO-t fog kérni RBTelkom-tól.
Általában az account összekapcsolás részeként, létrehoznak valamilyen hosszú távú/állandó információt, mint egy http cookie például, amely ennek a felhasználónak az identitásszolgáltatójaként azonosítja RBTelkom-ot. A roll-over időszak alatt ezt arra is használják, hogy megkülönböztessék a már összekapcsolt és „még nem összekapcsolt" felhasználókat. Amint a roll-over periódus befejeződött minden felhasználót aki nem rendelkezik ezzel az állandó információval, meg kell kérdezni, hogy eldöntsék, hogy RBTelkom e a valódi identitásszolgáltatójuk.

Where Are You From? (WAYF)

Néhány szolgáltatónak több identitásszolgáltatóval is lehetnek bizalmi kapcsolatai. Ez azt jelenti, hogy a felhasználó kezdeményezhet SSO-t az egyik IdP-től. A tartalomszolgáltató számára, azt az eljárást, amellyel meghatározza, hogy melyik IdP-től kell kérnie a SSO-t, Where are you from? (WAYF) szolgáltatásnak nevezzük. Ez egy olyan eljárás, ami által egy felhasználó meghatározhatja a preferált IdP-jeit. Ezt az információt a SP kezeli, így egyszerűen – felhasználói beavatkozás nélkül – meghatározhatja, hogy a jövőben melyik IdP-től kell kérnie a SSO-t.
RBBanking ügyében, a WAYF információt a roll-over időszakban hozzák létre. Ebben a periódusban, RBBanking mind tartalomszolgáltatóként (a már szövetségi felhasználók

[6] Egy adott pozíció, szolgáltatás lejáratkori lezárása és egyidejű megújítása további időszakokra.

számára), mind identitásszolgáltatóként viselkedik (a nem federációs felhasználóknak). Vagyis RBBanking és RBTelkom is identitásszolgáltatóként viselkedik, az egyetlen tartalomszolgáltatónak RBBanking-nak.

Ha RBBanking egyetlen SP volna több IdP-nek, akkor támaszkodnia kellene valamilyen állandó információra a felhasználóval kapcsolatban (mint például http cookie), hogy azonosítsa, hogy egy SSO kérést melyik identitásszolgáltatónak kell elküldeni. Ha a cookie hiányzik, akkor RBBanking-nak kezdeményeznie kell, valamilyen felhasználó általi WAYF feldolgozást. RBBanking úgy dönthet, hogy arra kéri Józsefet, hogy válasszon ki egy identitásszolgáltatót az ismert/megbízható IdP-k listájáról.

Némely esetben a tartalomszolgáltató nem hajlandó, felfedni a megbízható IdP-k listáját. Ekkor RBBanking utasítást adna Kiss úrnak, hogy miként érheti el közvetlenül az identitásszolgáltatóját (RBTelkom) és hogyan kezdeményezhet SSO kérést egy IdP alapú mechanizmuson keresztül.

Amíg ez valamilyen szinten a felhasználó együttműködésével jár, mégsem olyan tolakodó, mint az, hogy a felhasználónak kelljen emlékeznie a RBBanking-nál lévő jelszóra. Ideális esetben, a felhasználó-interaktív WAYF feldolgozást nem kellene minden alkalommal igényelni, amikor József hozzáfér RBBanking-hez.

Session menedzsment és hozzáférési jogosultságok

Amint a felhasználó egyszeri bejelentkezett egy tartalomszolgáltatóhoz, a SP felelős azért, hogy kezelje a felhasználó helyi munkamenetét. Ebbe beletartoznak a felhasználó cselekvéseivel kapcsolatos jogosultsági döntések és a munkamenet-kezelés maga, továbbá a kijelentkezés és a biztonsági időkorlát lejárta (session time-out).

Ez azt jelenti, hogy a SP képes kezelni a felhasználó attribútumait és bejelentkezési adatait valamilyen szinten. Ezeket az attribútumokat arra használják, hogy egy felhasználó helyi hozzáférési jogait meghatározzák. Hozzáférési jogokat az IdP adhat ki, a felhasználóról szóló kibocsátott (asserted) attribútumok formájában, ilyen például a csoporttagság.

Kijelentkezés

Néhány szövetségi forgatókönyvben, a globális kijelentkezés elképzelése (egyetlen kijelentkezés) szintén szükséges, lehetővé téve a felhasználónak, hogy egy IdP által kijelentkezési kérést küldjön minden munkamenethez. Globális kijelentkezést kérhet a felhasználó IdP-től és SP-től is, a globális kijelentkezés folyamatát az identitásszolgáltató

irányítja. Az IdP felelős azért, hogy kezelje azon SP-k listáját, akikhez a felhasználó az adott munkamenetben SSO-val bejelentkezett. Az IdP ekkor egy kijelentkezés-kérést fog küldeni mindezeknek SP-knek a felhasználó nevében.

Ez például úgy lehet, ha például József kijelentkezik RBTelkom portáljáról, RBTelkom már nem hajlandó, figyelembe venni azokat a tranzakciókat, amibe József belekezd. Ebben az esetben RBTelkom el fog indítani egy kijelentkezési kérést minden üzleti partnernek, amihez egy SSO kérést bocsátanak ki József aktuális munkamenetén belül.

A globális kijelentkezés nem utal arra, hogy a helyileg is kijelentkezés történik. Lehetséges az, hogy egy felhasználó ki kíván jelentkezni egy tartalomszolgáltatónál lévő munkamenetből, anélkül, hogy az IdP-nél lévő munkamenetet megszakítaná. Vegyük figyelembe, hogy ez azt igényli, hogy a felhasználó érti és ismeri a szövetség természetét és működését. Valószínűbb alternatíva egy SP-nél levő helyi kijelentkezésre, hogy rövidebb munkamenet össz/inaktivitási időtúllépés keretet kell beállítani, mint az alapértelmezett közvetlenül hitelesített munkamenetben. Egy rövidebb tétlenségi időtúllépés, az SSO felhasználónak elfogadhatóbb lehet, mivel így nem kényszerítik explicit újra hitelesítésre. Helyette, a SP egyszerűen újra kér egy SSO-t a felhasználó identitásszolgáltatójától.

Bejelentkezési adatok eltakarítása

A kijelentkezés, legyen az globális vagy helyi, gyakran magába foglalja a session megszakítását az SP-nél. Ez a munkamenet független lehet a kiszolgáló oldali alkalmazásokkal rendelkező munkamenetektől. A kiszolgáló oldali alkalmazás munkameneteit arra használhatják, hogy fenntartsanak egy státuszt a több lépésből álló tranzakciók kérés/válaszai között. Kijelentkezéskor, biztosítani kell, hogy mind az identitásszolgáltatónál, mind a tartalomszolgáltatónál mindenféle sessiont és az ahhoz tartozó attribútumokat megsemmisítik.

Nézzük meg mi történik, amikor József kijelentkezik a RBTelkom portálról és ezzel egyúttal a RBBanking weboldaláról. Ha József elindított egy tranzakciót (eszközök átvitelére például) aztán elfelejtkezett róla, akkor ezt a tranzakciót el kell takarítani (ez lényegében, egy szemétgyűjtő). Ha ez nem történik meg, akkor RBBanking-nek olyan árva munkamenetei maradnak, amik erőforrásokat köthetnek le a kiszolgáló oldali alkalmazásainál.

Globális good-bye

A globális good-bye kezeli a felhasználó hozzáférési jogainak és felhatalmazásainak visszavételét egy szövetségi forgatókönyvön belül. Akkor használják mikor egy IdP és SP közti kapcsolat megszűnik, minden felhasználói attribútum (beleértve a tranzakció, profil és szolgáltató specifikus attribútumokat) ami fontos a megszűnő kapcsolat szempontjából, szintén megszűnik. Vegyük figyelembe, hogy a szövetségi kapcsolatok többféle módon befejeződhetnek: A felhasználó úgy dönthet, hogy megszakítja a kötését az IdP és a SP között vagy az identitásszolgáltató és a tartalomszolgáltató nem kívánja folytatni az együttműködést, így megszakítva az IdP felhasználóinak kötéseit.

Például, ha a kedvenc alkalmazottunk, Első úr új állás után néz (és a KisCég-nél dolgozik ezután) akkor hozzáférési jogait és jogosultságait és NagyCég által szponzorált utazási kedvezményeit el kell távolítani, a NagyCég és RBTravel közti globális good-bye részeként. Megjegyzendő, hogy ez nem jelenti azt, hogy eltávolítanák Első úr accountját - beleértve a szolgáltató specifikus attribútumokat – RBTravel-nél. Ez csak annyit tesz, hogy minden NagyCéggel kapcsolatos attribútumot (beleértve a tranzakció és profil attribútumokat) törölnek Első úr RBTravel accountjából.

Általában a globális good-bye az account szétkapcsolással együtt megy végbe.

Account szétkapcsolás

Az account szétkapcsolás az az eljárás, amely a közös egyedi azonosítót megsemmisíti, megszüntetve annak a lehetőségét, hogy az IdP és SP egyedileg utaljon egy adott felhasználóra. A szétkapcsolás egyik eredménye, hogy a felhasználó már nem használhatja az egyszeri bejelentkezést IdP-től az SP felé. Megjegyzendő, hogy az account szétkapcsolás független attól, hogy az SP-nél miként hozták létre az accountot/regisztrációs bejegyzést, tehát a szétkapcsolás lehetséges akkor is, ha az accountot explicit létrehozta a felhasználó vagy az IdP, SP provisioning eredményeként jött létre. A szétkapcsolás után a felhasználó vagy a SP választhat egy másik IdP-t az account összekapcsolás céljából, vagy a tartalomszolgáltató úgy dönthet, hogy folytatja a user közvetlen hitelesítését.

Kiss József dönthet úgy, hogy megszünteti RBTelkom-os számláját. Ez történhet költözés miatt vagy, mert szolgáltatót vált stb.. Esetünkben József már nem lesz képes SSO-val elérni RBBanking-ot RBTelkom-tól, mert már RBTelkom-hoz sem fog tudni belépni. Ebben az esetben József információit RBTelkom-nál és RBBanking-nél is szét kell kapcsolni („de-

federálni”). A folyamat eredményeként a József közös egyedi azonosítóját megsemmisítik, és az egyszeri bejelentkezési képességét RBTelkom-nál elveszti, továbbá visszahelyezik olyan felhasználónak, akit közvetlenül hitelesít RBBanking.

Összefoglalás

Mint az látható, a piac minden szférájában – a fennmaradás érdekében – szerkezeti átalakulás várható illetve tapasztalható. Ahhoz, hogy egy vállalat minél inkább az adott termék vagy szolgáltatás minőségi előállítására tudjon koncentrálni, a nem létfontosságú részegységeket más cégekhez, szolgáltatókhoz szervezik ki, ezáltal egy érték hálót létrehozva. Azonban, hogy a vállalat továbbra is fennakadás nélkül folytathassa tevékenységét, szükséges a szövetségek létrehozása. A federáció lehetővé teszi a felhasználóinak az erőforrások akadálymentes elérését, legyen az akár teljesen különböző biztonsági tartományban, továbbá a felhasználók kezelésével és hitelesítésével kapcsolatos tevékenységet egy adott szolgáltatóra hárítja ez által is csökkentve a vállalat költségeit, és növelve a biztonságot. Ennek a „kényelemnek” az ára a bizalom és a megbízhatóság. A szövetségi azonosítás alapjául többféle szabvány is szolgál, és jelenleg több nagyvállalatnak is vannak saját implementációi erre a problémára.

Források:

- IBM Redbooks - Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions
  http://www.redbooks.ibm.com/abstracts/sg246394.html
- Lantos Ádám - Web-alapú identitás federáció
  https://redmine.kirdev.sch.bme.hu/attachments/92/identityfederation-v06-adam.lantos.pdf
- Wikipedia – SAML cikke (angol nyelvű)
  http://en.wikipedia.org/wiki/SAML
- Nemzeti Információs Infrastruktúra Fejlesztési Program AAI Projekt
  https://wiki.aai.niif.hu/index.php
- [1] Idézet - http://lists.oasis-open.org/archives/security-services/200101/msg00014.html