ÜGYFÉLKAPU AZONOSÍTÁS HASZNÁLATA OKTATÁSI KÖRNYEZETBEN

Szerzők

Roskó Tibor
Debreceni Egyetem

Adamkó Attila
Debreceni Egyetem

Első szerző e-mail címe:
r.tibor92@gmail.com

Lektorok

Kusper Gábor
Eszterházy Károly Egyetem

Márien Szabolcs
InnovITech Kft.

Szilágyi Barnabás
Debreceni Egyetem

Nemes Magdolna
Debreceni Egyetem

Roskó Tibor és Adamkó Attila (2016): Ügyfélkapu azonosítás használata oktatási környezetben. *Különleges Bánásmód*, II. évf. 2016/4. szám, 81-94. DOI 10.18458/KB.2016.4.81

Absztrakt

Cikkünkben a központosított oktatáshoz kapcsolódva egy új oktatási azonosító bevezetésének lehetőségét szeretnénk bemutatni. A megoldásunkhoz korábbi kutatásaink eredményei szolgáltatták az alapot. Célunk nem kizárólagosan elvetni a már meglévő törekvéseket, mint például az eduID szolgáltatás, hanem elsőként egy már működő infrastruktúra bevonásának lehetőségét megvizsgálni, másodsorban pedig egyfajta továbbfejlesztési irányt mutatni az említett eduID tekintetében.

Az elkészített tanulmányunkban megfogalmazott hipotézisek alátámasztását egy felméréssel kívánjuk alátámasztani, mely nagymértékben igazolja is feltételezéseinket.

Kulcsszavak: ügyfélkapu, oktatási azonosító, debreceni egyetem, eduID

Diszciplínák: Informatikai tudományok

Abstract

USE OF CLIENT GATE FOR IDENTIFICATION IN EDUCATION ENVIRONMENT

In our article we would like to describe a possible implementing of a new education ID which is related to centralized education. Our solution is based on results of our other researches. The goal is not to reject directly previously created solutions, like eduID, instead of it first we would like to inspect the opportunity to use well designed infrastructures, secondary we would like to give a future plan for extending eduID.

In our paper we drew up some hypotheses which should to be confirmed, so we created a survey. This completely confirmed almost our all hypotheses.

Keywords: client gate, education id, university of debrecen, eduID

Disciplines: Computer Science

Napjaink és a jövő informatikájában nélkülözhetetlen az automatikus adatfeldolgozás, ennek alapja, hogy az információ gépek számára is megérthető formában keletkezzen. A szemantikus web alapkövetelménye, a dokumentumok olyan metaadatokkal való ellátása, mely által a számítógép valódi tartalomként tudja kezelni, ugyanazt látja egy információhalmazban, mint egy ember.

A FOAF (Friend Of A Friend), mint digitális névjegykártyaként történő alkalmazásának megvalósítására létrehozott projektünk áll ehhez legközelebb azáltal, hogy itt egy személyt leíró adatstruktúrát jelenítünk meg gépi feldolgozhatóságot biztosítva.

A tanulmányban részletesen ismertetni kívánt téma egy dokumentum hitelesítő megoldásból nőtte ki magát. E program keretében az elektronikus aláírással egyenértékűen megbízható, bizonyos kereteken belül -belső adatkezelés során- vele közel egyenértékűnek tekinthető megoldást szeretnénk megvalósítani, mely a PDF/a XMP (Extensible Metadata Platform) metaadataira és az ügyfélkapu személyhitelesítő szolgáltatására épülve biztosít lehetőséget egy dokumentum hitelesítésére.

Az ügyfélkapu szolgáltatásának további hasznosításából kiindulva jutottunk el a megvalósítandó célunkhoz, melynek során országos szintű, központi oktatási azonosító bevezethetőségét szeretnénk megvizsgálni, amely az ügyfélkapu funkciójára épülne. Tekintettel arra, hogy számos oktatási intézmény működik az országban, jelentős előrelépést nyújthatna egy központosított azonosítási rendszer bevezetése, melynek során minden -az intézménnyel kapcsolatban álló személy- egyetlen felhasználói fiókkal azonosíthatná magát, függetlenül az intézményektől.

Tanulmányunkban a fentiekben felvázolt megoldást szeretnénk részletesen körüljárva bemutatni a jelenleg működő rendszer előnyeit/hátrányait, magát az ügyfélkapu rendszert, a ráépülő azonosítási módszer előnyeit/hátrányait, mindezeket alátámasztva egy -a tanulmány pontosabb összképéhez elkészített- reprezentatív felméréssel, esettanulmánnyal.

Az elkészített tanulmány kapcsolata a különleges bánásmódot igénylő emberekkel sokrétűen meghatározható, jelen esetben egy kiemelkedő pozitívummal szeretnénk ezt leírni. Ez nem más, mint a negatív vagy bármilyen egyéb hátrányos diszkrimináció kizárásának biztosítása, melyet a bemutatni kívánt rendszer is támogat. Korábbi ismereteink szerint a speciális bizonyítványt szerzett személyek speciális, megjelölt bizonyítványt kaptak, mely a mai szemléletünkben diszkriminatív álláspontot követ, ezzel szemben napjainkban ilyen jelzés nem kerül rögzítésre okmányokban. Az ügyfélkapu rendszerben sem kerül ilyen információ tárolásra, illetve továbbításra a szakrendszerek felé, ezáltal kijelenthető, hogy nem hordoz diszkriminatív jegyeket. Ezen felül maga az oktatási környezet amelyben alkalmazhatjuk, lehet kizárólag a különleges bánásmódot igénylő tanulók adatait, tanulmányi létüket követő rendszer.

Jelenleg használt azonosítási megoldás: LDAP

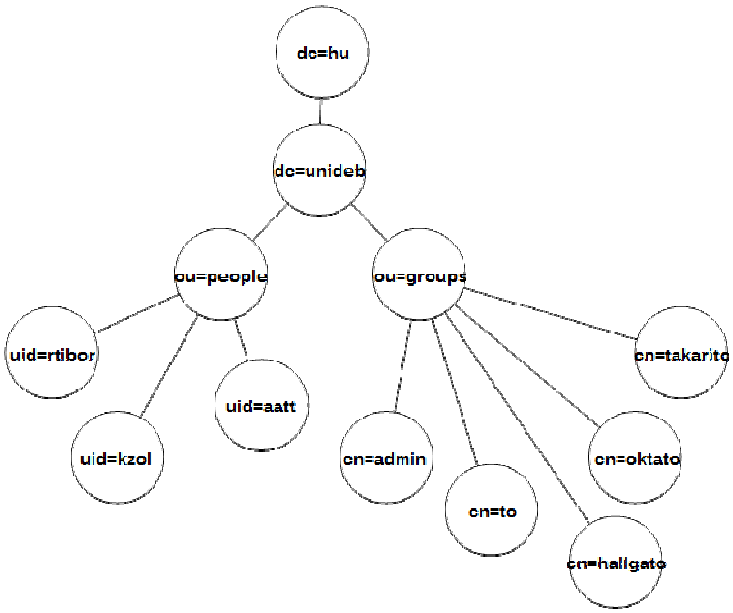
Az LDAP a Lightweight Directory Access Protocol (Egyszerűsített Címtárhozzáférési Protokoll) rövidítése. Az LDAP egy gyorsan kereshető fa struktúrájú adatbázist valósít meg, melyben viszonylag kevés a módosítás, ezáltal a keresésre lett optimalizálva. A rendszer nyílt forráskódú, szabadon elérhető bárki által. Működése során az információkat egy fában jeleníti meg és egy leíró séma alapján értékeli ki. Erősen objektum orientál, jól strukturált, osztályokból felépülő adatstruktúrát implementál.

A fa alulról felfelé történő olvasásával építhetünk fel egy LDAP lekérdezést, mely alapján az autentikáció létrejöhet, azaz visszaigazolja a lekért paraméterek meglétét.

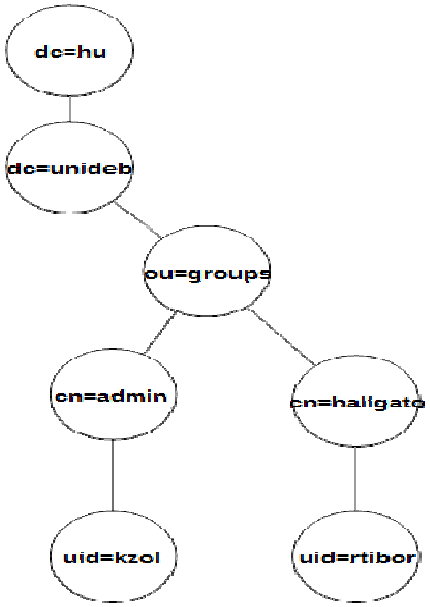
Az 1. ábrán láthatjuk, unideb.hu/people/kzol alakú hivatkozás jön létre. A 2. ábra bemutatja a kiválasztott személy mely csoport tagja, jelen esetben admin. Ezáltal a jogosultság kezelő

rendszer kzol részére az unideb.hu-hoz tartozó alrendszerekre az admin csoportnak engedélyezett műveletek végrehajtását fogja jóváhagyni.

1. ábra: LDAP fa (forrás: a Szerző)



2. ábra: LDAP jogosultságok (forrás: a Szerző)



Az LDAP-ban tárolt adatokat ldif (LDAP Data Interchange Format) formátumban tudjuk lekérdezni, melyre két példát szeretnénk ismertetni a fentebbi ábrákhoz kapcsolódva. Az első kódrészlet az admin csoport tulajdonságait írja le, illetve a hozzá tartozó személyeket is megjelöli:

```
dn: cn=admin,ou=groups,dc=unideb,dc=hu
objectClass: groupOfNames
objectClass: top
cn: admin
member: uid=kzol,ou=people,dc=unideb,dc=hu
member: uid=elmo,ou=people,dc=unideb,dc=hu
description: Admins group
```

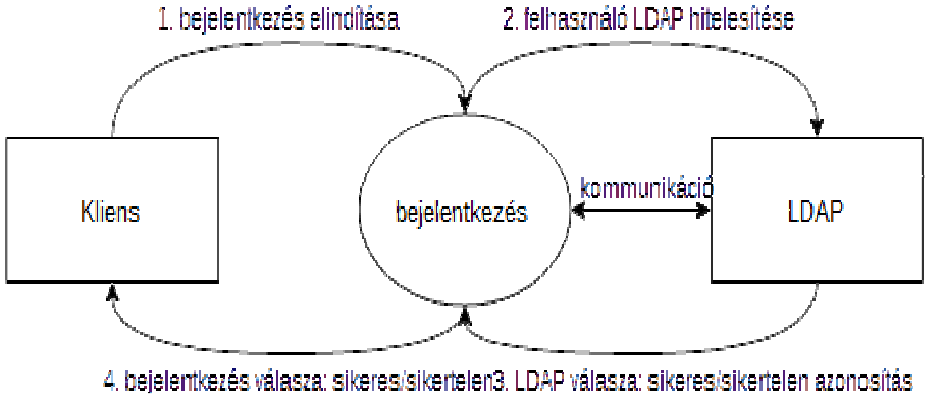
A következő adatsor a kzol azonosítójú alkalmazottat írja le. Az attribútumok közül az inetorgperson-t szeretnénk kiemelni, ez segít egy személyt hozzákapcsolni egy szervezeti egységhez, illetve lehetőséget biztosít jelszó megadására kódolt formában. A jelszót a userPassword attribútum tárolja a unicodePwd által kódolt formában.

```
dn: uid=kzol,ou=people,dc=unideb,dc=hu
objectClass: person
objectClass: top
objectClass: inetorgperson
objectClass: organizationalperson
cn: Kovács Zoltán
sn: Kovács
description: Vezető admin az egyetemen
employeeNumber: 18001
givenName: Zoltán
homePhone: +36701541287
l: Debrecen
uid: kzol
userPassword:: mvVlgpV1H
```

Mindkét kódrészlet a dn (distinguished name: egyedi, megkülönböztetett név) sorral kezdődik, ez reprezentálja az adott információ azonosítóját, ez a legmélyebben fekvő csúcs a fában, a hozzá vezetőt utat írja le egy globálisan egyedi azonosító formájában.

A 3. ábra alapján látható, hogy az azonosítás két lépésből tevődik össze: a kliens elindítja a bejelentkezést, rendszerint felhasználónév-jelszó megadásával és az LDAP rendszer visszaigazolja, hogy a megadott páros érvényes-e. Ezen felül szükséges lehet egyéb információk lekérdezése az azonosító rendszertől, például jogosultság, mely a Debreceni Egyetem esetén egy csoport tagság azonosítót takar.

3. ábra: LDAP azonosítás (forrás: a Szerző)



A Debreceni Egyetemen minden hallgató és alkalmazott rendelkezik hálózati azonosítóval, ez rendszerint egy felhasználónév és az ehhez tartozó jelszó. Ennek segítségével tudja igénybe venni az intézmény szolgáltatási rendszereit: Neptun, Eduroam, Kollégiumi adminisztráció, DEA. Minden szolgáltatás a bejelentkezési folyamatban kapcsolatba lép az LDAP szerverrel, amely visszaigazolja, a megadott felhasználónév-jelszó érvényes-e, valamint a jogosultság meghatározását is a szerver végzi. Ennek során a felhasználóhoz rendelt csoport tagság azonosítóját, csoportnevet adja vissza az LDAP, majd egy különálló jogosultságokat kezelő rendszer igazolja vissza, a felhasználó jogosult egy adott alkalmazás használatára. Ebben a nyilvántartásban kezeli az Egyetem minden kiosztott csoport jogosultságát az elérhető szolgáltatásokra nézve. Egy felhasználó több különböző csoport tagja is lehet, ezáltal eltérő jogosultságok birtokosa lehet minden alrendszer esetén.

Előnyök:

1. Nyílt hozzáférésű, térítésmentes: bárki számára térítésmentesen elérhető, felhasználható azonosítás elvégzésére.
2. Fa struktúrájú: szemantikus webre jól illeszthető, gráfhoz közel álló adatstruktúrát valósít meg. Ezáltal a keresés, adatlekérdezés hatékonyan megvalósítható.

Hátránya: a lokális, intézményen belüli azonosítás. Vagyis legfőbb hátránya, hogy a szolgáltatás rendszerint intézményen belül érhető el, ezáltal mindenhol eltérő felhasználói fiókokat kell kezelni mind a rendszerekben, mind a felhasználónak.

Megemlítettük a helyi azonosítót, mely minden egyetemi személyhez hozzá lett rendelve, ez nem más, mint az eduID. Hasonlóan az ügyfélkapuhoz, ez is egy kormányzati megoldás, viszont itt szabványosított azonosító használatához kapunk előírásokat, megszorításokat, nem egy autentikációs alkalmazást jelent. A SAML2 protokollon alapul, melynek célja SSO bejelentkezés használata, egyszer kell bejelentkezni egy munkamenet során, hasonlóan, mint az ügyfélkapu esetén.

A csatlakozó intézmény helyileg hozza létre a felhasználói bázist, minden személy megad egy felhasználónév-jelszó párost. A létrehozott autentikációs adatbázisból oktatási egységen belül azonosíthatja magát bárki, ezen túlmenően az eduID-t használó szervezetek alkalmazásaiban is lehetőség nyílik a honintézmény által történő beazonosításra.

A fent leírt megoldás bármely szolgáltató által igénybe vehető, mint kihelyezett bejelentkezési, azonosítási megoldás. Az eduID bejelentkezés során azonosítja magát az adott személy a szolgáltató felé, illetve átadásra kerülnek a szükséges attribútumai, legfontosabbak a jogosultságot leírók.

Előnyök: központosított azonosítás. A honintézmény kezeli a bejelentkezéshez szükséges felhasználónév-jelszó párost. Lehetőség van a kihelyezett azonosításra, melynek során a honintézmény azonosítja be a felhasználót egy szolgáltatónál. Ezáltal nincs szükség további regisztrációkra intézményen belül, illetve külső szolgáltatók esetén.

Hátrányok:

1. Intézmény szinten kezelni kell a felhasználót: biztosítani kell intézményen belül egy azonosító rendszert, amely bejelentkezteti a felhasználót, illetve azonosítja külső szolgáltatás felé. Nem valósul meg az egy fiókos bejelentkezés, ha több intézményben is érintett.
2. Nincs visszavezetett kijelentkeztetés: több külső szolgáltatás tesztelésekor sehol nem találtunk lehetőséget kijelentkezésre, ezáltal a biztonság nagyban megkérdőjelezhető. A munkamenet csak a böngésző lezárásával szüntethető meg. Erre az ügyfélkapu rendszer esetén nem csak lehetőség van, de kötelező is biztosítani minden szolgáltató részéről a kijelentkezés lehetőségét.

Mi az ügyfélkapu rendszer?

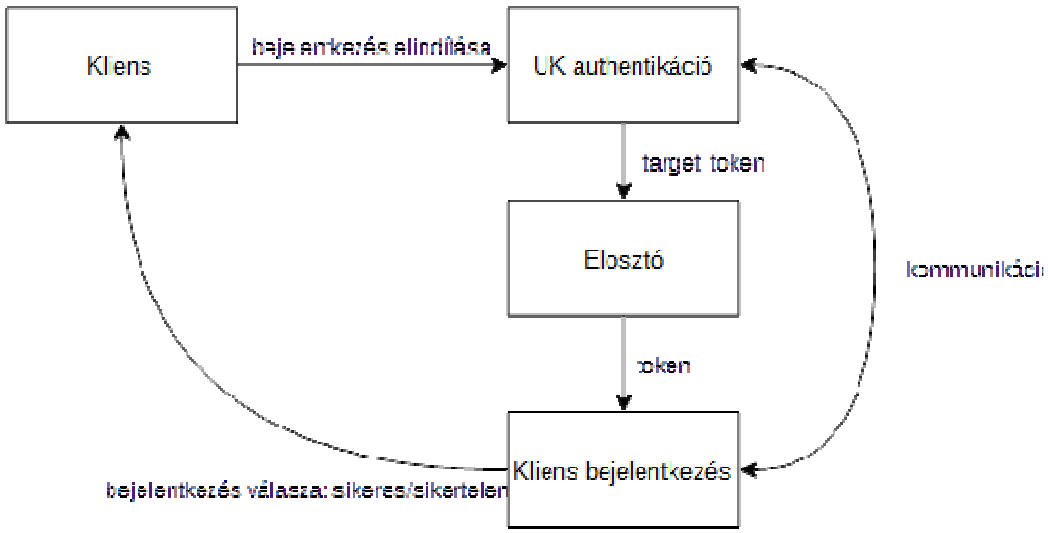
Az ügyfélkapu a magyar közigazgatás elektronikus formába történő konvertálásának alapja, mely a www.magyarorszag.hu címen érhető el. Bevezetésével a kormány célja a lakosság ügyintézésének elektronikus formában történő megvalósulásának elősegítése volt, napjainkban szinte minden papír alapon elérhető ügyintézés online felületen is megvalósított, ezen felül számos nyilvántartás ilyen formában valósul meg, például az anyakönyvek vezetése. Köszönhetően az elektronikus aláírás megjelenésének, ma már az online elindított ügyek bármelyike lefolytatható kizárólag papírmentes formában is, például egy lakás adásvétel. Tekintettel az e-aláírás költségeire, még számos szolgáltató, illetve polgár nem rendelkezik a szükséges eszközökkel, emiatt a papír még mindig meghatározó az ügyek intézése során.

Ügyfélkaput bármely magyar állampolgár igényelhet, aki tudja igazolni személyazonosságát, például személyi igazolvánnyal. Térítésmentesen vehető igénybe minden szolgáltatása, melybe nem tartozik bele az esetleges járulékfizetés, illetékek esetén.

A közszférában működő hivatalok, intézmények részére biztosít többletszolgáltatásokat is a rendszer. A tanulmányban bemutatásra kerülő azonosítási módszer is ilyen többletszolgáltatásra épülve valósul meg. Két ilyen szolgáltatást említenénk meg: személy azonosítás, viszont azonosítás. Az első esetben egy személy bejelentkezése után annak neve, e-mail címe és regisztrációjának státusza kérhető el az ügyfélkapu nyilvántartásból. Második esetben az előzőeken felül lehetőség van ismert okmányazonosítók érvényességének ellenőrzésére, illetve a személyhez tartozás ellenőrzésére. Részünkre az első szolgáltatás mérvadó azáltal, hogy a személy e-mail címe egyedien tud azonosítani, a lokális jogosultságkezelés elvégezhető vele, illetve csak azon személyeket engedélyezzük, akik véglegesített regisztrációval rendelkeznek.

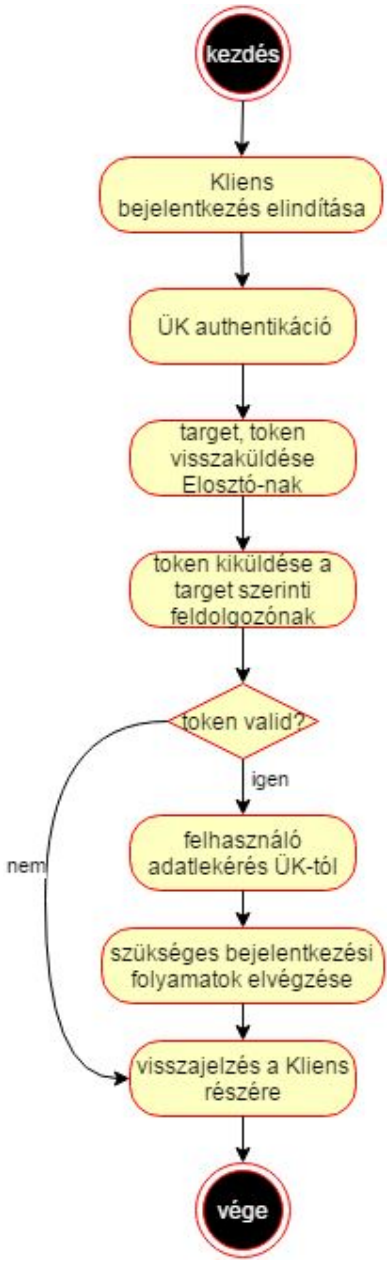
A 4. ábra bemutatja az ügyfélkapu autentikáció folyamatát, mely alapjaiban nem tér el az LDAP rendszertől. A megjelenő fő különbség, hogy itt több lépcsőt jár be az azonosítás mire visszajut a válasz a kliens részére. Ezen felül a jogosultság megállapítása a Kliens bejelentkezés komponensben valósulna meg a korábban használt jogosultság kezelő rendszerrel. Ez alapján az azonosítást az ügyfélkapu, míg a jogosultság kiosztást lokálisan működő szolgáltatás végezné el, megvalósítva a központi, egy felhasználói fiókos azonosítást.

4. ábra: ügyfélkapu (ÜK) azonosítás (forrás: a Szerző)



Az 5. ábra kibontva mutatja be az azonosítási folyamatot, melynek során a Kliens bejelentkezés komponensben hajtódik végre a visszakapott token hitelességének ellenőrzése, illetve felhasználásával kérhető el a személy adathalmaza. Amennyiben sikertelen a token ellenőrzése, az azonosítási folyamat sikertelen, a végrehajtás megszakításra kerül.

5. ára: ügyfélkapu (ÜK.)azonosítás algoritmusa (forrás: a Szerző)

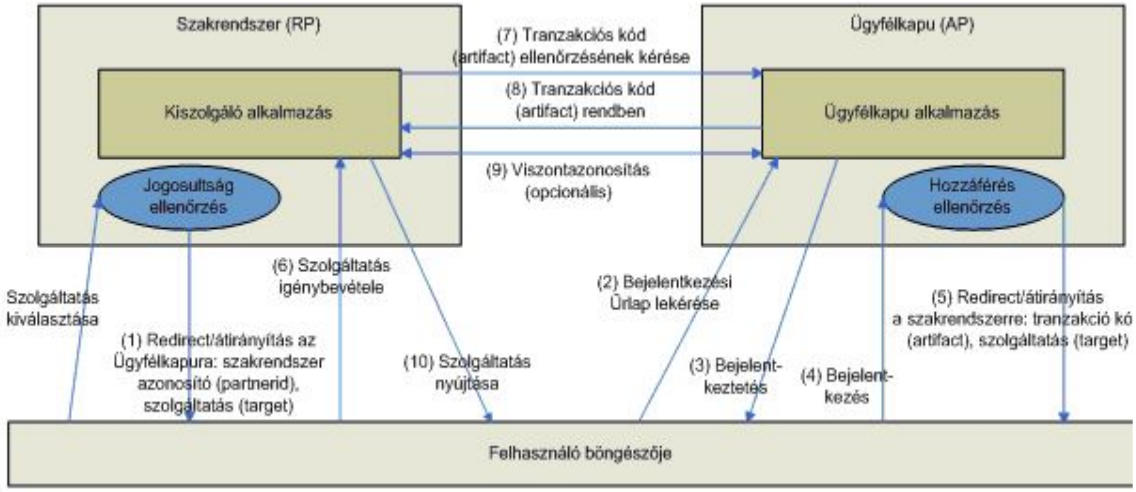


Az azonosítás használatához intézményi csatlakozás szükséges a központi SSO (Single Sign-On) modulba. Erre lehetőség a közigazgatás szerveinek, illetve nonprofit szervezeteknek

biztosított, illetve engedélyezett. A Nemzeti Infokommunikáció Szolgáltató Zrt. visszajelzése alapján a Debreceni Egyetem, mint oktatási intézmény csatlakozhat a rendszerbe. Ebből kiindulva a hazai iskolák igénybe vehetik a szükséges szolgáltatást, így kiépíthető országos szintű, központi azonosításon alapuló rendszer. Az intézmények részéről vezetői igénybejelentésre, valamint a működéshez nélkülözhetetlen eszközök biztosítására van szükség.

A 6. ábrán szemléltetjük az adatcsere folyamatát a kiszolgáló rendszer és az ügyfélkapu között.

6. Ábra: Szakrendszer - ÜK kommunikáció (forrás: KIB.21.ajánlás)



Előnyök:

1. Központi azonosítást tesz lehetővé: a megoldás fő előnye, hogy országos szinten egy felhasználói fiókkal érhető el az ügyfélkapu minden szolgáltatása és az erre ráépíthető további megoldások halmaza, jelen esetben az oktatási azonosító.
2. Térítésmentesen használható: a szolgáltatás térítésmentesen vehető igénybe, illetve térítésmentesen használható személyazonosítás céljából.

Hátrányok:

1. Korlátozott elérhetőség. Ez abból adódik, hogy kizárólag közigazgatási vagy nonprofit szervezetek vehetik igénybe, külön engedélyhez kötve. A megvalósítandó elképzelésünkhöz, azáltal, hogy oktatási környezetben kívánjuk használni, problémamentesen hozzáférhető, így jelen esetben nem tekintendő negatív esetnek e tulajdonság.
2. Biztonságkritikus rendszer: azáltal, hogy eleve egy komplex szolgáltatási körrel rendelkező rendszerbe kapcsolódunk egy viszonylag ugyancsak komplex rendszerrel magas biztonsági kockázatot hozunk be, mint nem elhanyagolható tényező. A később elemzendő felmérésben is megjelenik erre irányuló aggály, viszonylag csekély mértékben, de ettől függetlenül kiemelt prioritással kell a biztonságot szem előtt tartani. Egy korábbi tanulmányunkban is kitértünk a biztonság kritikus szerepére a jövő papírmentes ügyviteléhez viszonyulva.

A kockázatok mérséklése érdekében bevezethető az ügyfélkapu rendszerhez többlépcsős bejelentkezési folyamat, melynek során a felhasználónév-jelszó megadását követően, például sms kódot küld a rendszer, melyet a felületen szükséges megadnunk, mint második szintű azonosító. Ilyen jellegű megoldásokat már több nemzetközi szolgáltató is alkalmaz, például a

Google. Az Ő esetükben további szintet is bevezettek, melynek során a felhasználónév megadását és ellenőrzését követően kéri be a jelszót a bejelentkeztető felület. A megoldást elemezve két megállapítást is tehetünk: magasabb a biztonsági szint azáltal, hogy a felhasználónév ismerete nélkül nem próbálgathatjuk a jelszavakat, viszont itt kiszivárgó adatként megjelenik, hogy az adott felhasználónév nem szerepel a rendszerben.

Ügyfélkapu bevezetésének lehetősége LDAP helyett

Az eddigi ismertetés után tekintsük át, milyen módon oldható meg, illetve milyen nehézségeket kell leküzdenünk az ügyfélkapu oktatási azonosító bevezetéséhez.

Az LDAP kiváltása egyszerűen kivitelezhető, a kliens részére kell megadni az új hitelesítő rendszer elérhetőségét. Természetesen ettől összetettebb feladatokat is meg kell oldanunk ahhoz, hogy a háttérrendszer ki tudja szolgálni a kliens bejelentkezését.

1. Létre kell hozni egy elosztó komponenst, mely az ügyfélkapu válaszát feldolgozva továbbküldi a token-t a megfelelő -target (célérték) szerinti- alrendszernek.
2. Létre kell hozni a kiszolgáló alrendszert, mely a bejelentkezés folyamatát végzi el, az ügyfélkapu token-el.

Az elosztó komponensben egyetlen végrehajtó parancs kezeli a kapott target-et, átküldi az ennek megfelelő alrendszerhez a token-t, meghívja a nyilvános interface-ét.

A kiszolgáló alrendszer jelen esetben a felhasználó bejelentkezését és jogosultságainak kiosztását hajtja végre. A korábban megemlített ügyfélkapura épülő dokumentum hitelesítő megoldásunk révén a token ellenőrzését, illetve a felhasználó adatait lekérő funkciókat nem szükséges újra implementálni azáltal, hogy a komponens alapú tervezés jóvoltából módosítás nélkül újrafelhasználhatók. Kizárólag a szabályokat érvényesítő modellt kell felépíteni, mely meghívja a korábban implementált függvényeket.

Felmerülő nehézségek és ezek megoldásai:

1. *Nincs mindenkinek ügyfélkapu regisztrációja.* Minden személy, aki rendelkezik személyazonosság igazolására elfogadott dokumentummal igényelhet ügyfélkapu fiókot. Ezáltal nem jelenthet fennakadást, hogy nincs mindenkinek felhasználói fiókja.
2. *Jelentős számban tanulnak/dolgoznak külföldi állampolgárok oktatási intézményekben.* A tájékoztató alapján bármely külföldi állampolgár igényelhet ügyfélkapu hozzáférést, aki tudja igazolni személyazonosságát.
3. *Hogyan történik a jogosultság kezelése?* A korábban működő rendszer jogosultság kezelő funkcióját megtartva, azt összekapcsolva a bevezetésre kerülő ügyfélkapu oktatási azonosítót kezelő alrendszerrel.

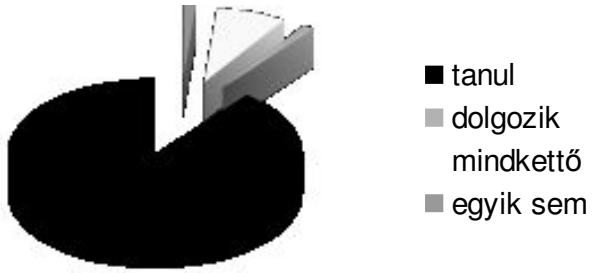
Miért lenne alkalmasabb az ügyfélkapu oktatási azonosító, mint például az LDAP használata?

A mi véleményünk alapján egy központi azonosító mindig felhasználható összetettebb feladatokra is, az eredeti funkciójától függetlenül. Ezt egy lokálisan kialakított azonosító esetén nem vagy nehezen kivitelezhető. Mindezek alátámasztására készítettünk egy felmérést/esettanulmányt, melynek során megkérdeztünk személyeket az ügyfélkapu oktatási azonosító bevezetésével kapcsolatban. Az alábbiakban ennek eredményét szeretnénk részletezni.

Az első mérési szempont, hogy a megkérdezett személy tanul vagy dolgozik oktatási környezetben, ez lehet múlt, illetve jelen idejű esemény is. Ez azért alapvető információ, mert elsődlegesen oktatási azonosításra kívánjuk bevezetni az ügyfélkapu rendszert, releváns választ pedig az tud igazán adni, aki maga is részese a jelenlegi azonosítók használatának.

A 7. ábrán megjelenő válaszok arányából élesen kitűnik, a legtöbben hallgatók. Ez a többi választ is meghatározza azáltal, hogy a kialakult képet a hallgatók szemszögéből vizsgálhatjuk, ez nem feltétlenül jelenthet problémát, a leginkább egyébként is a tanulók kerülnek kapcsolatba ezen azonosítók használatával, az ezekből adódó nehézségekkel, viszont a jövőben egy átfogóbb felmérést is szeretnénk elvégezni, amely intenzívebb módon kiterjed a teljes egyetemi emberi erőforrásra.

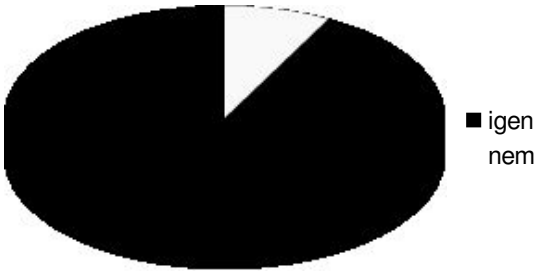
7. ábra: tanul-dolgozik megoszlás oktatási környezetben (forrás: a Szerző)



A 8. ábra egyértelműen megmutatja a válaszadók szinte mindegyike használ(t) központi, lokális azonosítót. Itt azon személyeket kérdeztünk meg, akik az előbbi kérdésben a tanul/dolgozik kategóriába tartoznak.

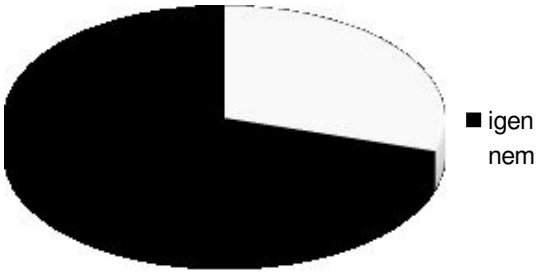
A kiugró érték nem meglepő, hiszen minden intézmény alkalmaz helyi, központosított azonosítókat, melyek a számítógépek, tanulmányi és egyéb információs rendszerek elérését biztosítják.

8. ábra: Használ(t) központi azonosítót kérdés alapján történő megoszlás (forrás: a Szerző)



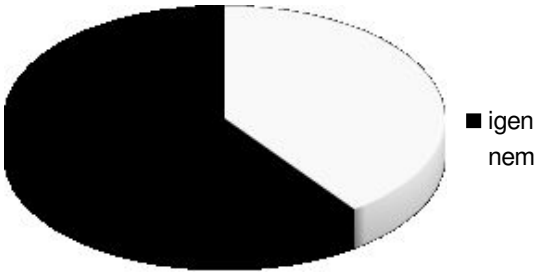
A soron következő kérdést a 9. ábra reprezentálja, mely ismét az 1. kérdésben szűrt személyekre vonatkozik. Itt azt mértük fel, milyen a megoszlása a több intézményt is megjárt személyeké, kiderült a több egységet is érintetteké a nagyobb szám. Ez alapján pontosabb képet kaphatunk a következő kérdésekről, szélesebb látókörrel rendelkeznek a mért egyedek az azonosítókat tekintve.

9. ábra: Érintett több oktatási intézményben (forrás: a Szerző)

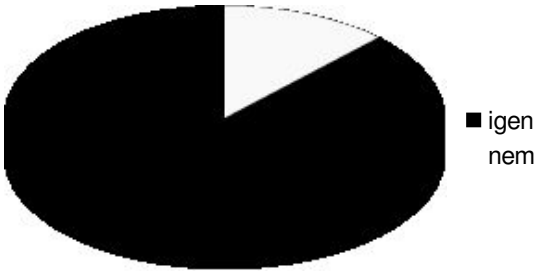


A 10. ábrán szerepeltetett kérdés alátámasztja azon feltételezésünket, hogy minden intézmény esetén külön azonosító használatába ütközünk, mely a következő kérdésben fel is tárja hiányosságait azáltal, hogy bár elenyésző számban, de akadt probléma ezek használata során. Ezt a 11. ábra mutatja be.

10. ábra: Szüksége volt eltérő azonosítókra (forrás: a Szerző)



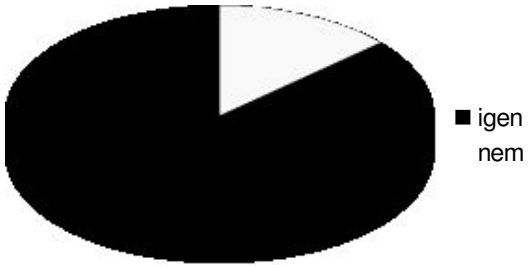
11. ábra: Adódott ezen azonosítókkal problémája (forrás: a Szerző)



A soron következő kérdés már a tényleges bevezetést készíti elő, megalapozó számadatot láthatunk a 12. ábrán, a megkérdezettek szinte mindegyike azon elképzelést támasztja alá, hogy a központi azonosító könnyítést jelenthet. A nemre szavazók esetében sem a könnyítés a

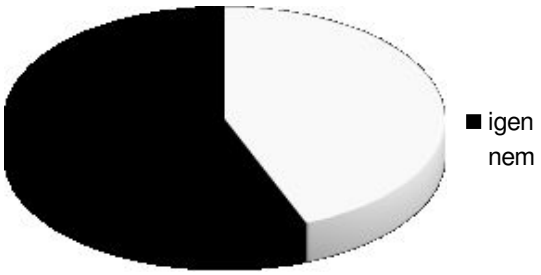
cáfolt állítás, egyszerűen nem szeretnének központosítani minden azonosítót. Ez a felmérés végén kapott szöveges válasz alapján leginkább biztonsági aggályok miatt áll fent. Ez tovább erősíti álláspontunkat, mely szerint a biztonságot kiemelt prioritással kell kezelni egy hasonló rendszer bevezetése és működtetése során.

12. ábra: Könnyítés lenne központi azonosítót használni (forrás: a Szerző)



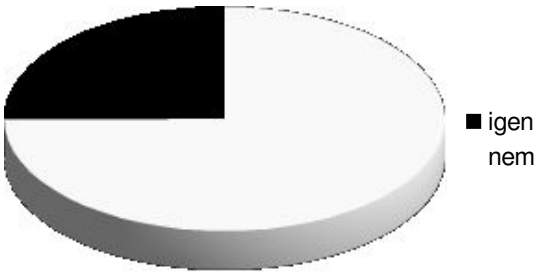
A következő kérdések az ügyfélkapura vonatkozóan gyűjtenek releváns információkat, a 13. ábrán reprezentált eredmény a válaszadók között érvényes ügyfélkapu fiókkal rendelkezők arányát mutatja be. Az eredmény szerint ez kicsivel több, mint 50%, ez tekintettel a behatárolható életkorra, jó eredménynek könyvelhető el.

13. ábra: Van érvényes ügyfélkapu regisztrációja (forrás: a Szerző)



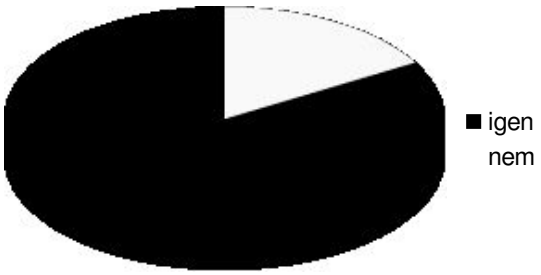
A 14. ábra eredménye viszont már nem mutat ilyen pozitív adatokat, az érvényes fiókkal rendelkezők csekély számban használják rendszeresen az ügyfélkapu szolgáltatásait. Viszont itt ismét figyelembe kell venni az átlagéletkort, mely alapján megállapíthatjuk, hogy nem feltétlenül kellene rendszeresen igénybe venni a rendszert, hiszen a fiatal korosztály ügyintézése nagyrészt kimerül a TB vagy adózási, illetve igazolványokhoz kapcsolódó ügytípusok kezelésével.

14. Ábra: Rendszeresen használja ügyintézésre az ügyfélkaput (forrás: a Szerző)



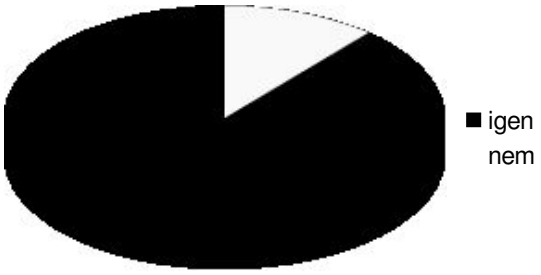
A 15. ábra annak arányát kívánja bemutatni, milyen számban regisztrálna az is fiókot, aki jelenleg nem rendelkezik vele, annak érdekében, hogy bizonyos ügyeinek intézése gyorsabb, kényelmesebb formában valósulhasson meg. Ez pozitívum számunkra is, hiszen az ügyfélkapun alapuló oktatási azonosító bevezetésével minden, az intézménnyel kapcsolatban álló személy részére szükségessé válna egy ügyfélkapu fiók regisztrálása. A kapott eredmények tükrében nem kell aggódnunk azon, hogy a résztvevők egyéb okok miatt nem regisztrálnának.

15. ábra: Ha nincs ügyfélkapuregisztrációja, regisztrálna a gyorsabb ügyintézés miatt? (forrás: a Szerző)



Az igazán releváns és fontos információt a 16. ábra által szemléltetett kérdés jelenti számunkra. Ezáltal ugyanis, szinte mindenki csatlakozna a központi azonosító használatához. Biztosak vagyunk benne, hogy a nemmel válaszolók esetén a magasabb biztonsági kritériumok, illetve biztosítékok megteremtése pozitív előremozdulást jelenthet, vagyis amennyiben tudjuk garantálni a hosszútávon is helytálló biztonságot, ők is becsatlakoznak a rendszerbe. Erre a szövegesen érkezett válaszokból következtettünk, melyek minden esetben a feltörhetőséget, biztonsági réseket emelték ki.

16. ábra: Csatlakozna ügyfélkapu oktatási azonosító használathoz? (forrás: a Szerző)



Összefoglalás

Mindenek előtt egy nagyon pozitív konklúziót tudtunk levonni az esettanulmányként elkészített felmérés keretében. Az általunk felvázolt hipotéziseket szinte maximálisan validálták az alanyok, váratlan eredmények, visszajelzések nem érkeztek.

Az elkészített tanulmány és ennek validálása révén elképzelhetőnek tartjuk az ügyfélkapu rendszer bevezethetőségét, mint oktatási azonosító. Illetve a cikkünkben bemutatott eduID ilyen módon történő továbbfejlesztése is rendkívül hasznos lehetne, ezáltal ha nem is ügyfélkapura épülve, de megvalósítható lenne egy központi, egy fiókos oktatási azonosító.

Ezen felül megszületett bennünk egy olyan absztraktabb szintre történő lépés is, melynek során nem csak az azonosítást, de a jogosultság kezelést is központosított rendszerbe lehetne integrálni. Ezáltal az intézmények még inkább tehermentesíthetőek lehetnének az adminisztráció szempontjából, csupán a szerepkörökhöz tartozó összepárosítást kellene elvégezni.

Bízunk benne, hogy az elkészített tanulmány hozzájárulhat egy egyszerűbb, kevesebb adminisztrációt igénylő, viszont maximális biztonságot, megbízhatóságot nyújtó oktatási azonosító rendszer létrehozásához.

Irodalom

Barrett, D.J. (2003). Linux Security Cookbook. O'Reilly.

Dhanjani, N., Clarke, J. (2005). Network Security Tools. O'Reilly Media, Inc. Letöltés: 2016. 06. 06. Web: https://books.google.hu/books?id=jYepAQAAQBAJ&hl=hu

EduID hivatalos weboldal. Letöltés: 2016.16.15. Web: http://www.eduid.hu/

Erl, T. (2009). Service Oriented Architecture. Prentice Hall.

Közigazgatási Informatikai Bizottság (2016. 05.). Hivatali Kapu Interfész Specifikáció. Letöltés: 2016. 06. 06. Web:https://ugyintezes.magyarorszag.hu/dokumentumok/kib_21.zip

OpenLDAP 2.4 dokumentáció. Letöltés: 2016. 06. 06. Web: http://www.openldap.org/doc/admin24/OpenLDAP-Admin-Guide.pdf

Sullivan, B. (2012). Web Application Security. McGraw-Hill.

Tuttle, S., Ehlenberger, A. (2006). Understanding LDAP Design & Implementation. IBM. Letöltés: 2016. 06. 06. Web: https://books.google.hu/books?vid=ISBN:9780738497860&redir_esc=y&hl=hu