ZAKLJUČNO POROČILO O REZULTATIH OPRAVLJENEGA RAZISKOVALNEGA DELA NA PROJEKTU V OKVIRU CILJNEGA RAZISKOVALNEGA PROGRAMA (CRP) »KONKURENČNOST SLOVENIJE 2006 – 2013«

I. Predstavitev osnovnih podatkov raziskovalnega projekta

1. Naziv težišča v okviru CRP:

Konkurenčno gospodarstvo in hitrejša rast (1.4 – ~~Informacijska družba~~)

2. Šifra projekta:

V2-0382

3. Naslov projekta:

Upravljanje z digitalnimi identitetami na Univerzi v Ljubljani

3. Naslov projekta

3.1. Naslov projekta v slovenskem jeziku:

Upravljanje z digitalnimi identitetami na Univerzi v Ljubljani

3.2. Naslov projekta v angleškem jeziku:

Digital Identity Management at University of Ljubljana

4. Ključne besede projekta

4.1. Ključne besede projekta v slovenskem jeziku:

Digitalna identiteta, upravljanje z identitetami, zasebnost, imenik

4.2. Ključne besede projekta v angleškem jeziku:

Digital identity, identity management, privacy, directory

5. Naziv nosilne raziskovalne organizacije:

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

5.1. Seznam sodelujočih raziskovalnih organizacij (RO):

6. Sofinancer/sofinancerji:

7. Šifra ter ime in priimek vodje projekta:

13982	doc. dr. Mojca Ciglarič

Datum: 23.4.2009

Podpis vodje projekta:

doc. dr. Mojca Ciglarič

M. Ciglarič

Podpis in žig izvajalca:

Rektorica
prof. dr. Andreja Kocijančič
po pooblastilu
dekan:

prof. dr. Franc Solina

II. Vsebinska struktura zaključnega poročila o rezultatih raziskovalnega projekta v okviru CRP

1. Cilji projekta:

1.1. Ali so bili cilji projekta doseženi?

- [x] a) v celoti
- [ ] b) delno
- [ ] c) ne

Če b) in c), je potrebna utemeljitev.

1.2. Ali so se cilji projekta med raziskavo spremenili?

- [ ] a) da
- [x] b) ne

Če so se, je potrebna utemeljitev:

2. Vsebinsko poročilo o realizaciji predloženega programa dela[1]:

V okviru projekta smo z Univerzo v Ljubljani zastavili sodelovanje za doseganje naslednjih rezultatov:

1. Analiza, primerjava in izbira sistema za upravljanje digitalnih identitet
2. Strategija prehoda na sistem za upravljanje digitalnih identitet
3. Načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
4. Priprava gradiv za uporabnike in skrbnike sistema
5. Objava izkušenj pri vzpostavljanju sistema

Ustrezno rezultatom smo projekt razdelili v pet odgovarjajočih faz:

1. Izdelava analize, primerjava in izbira sistema za upravljanje digitalnih identitet
2. Priprava strategije prehoda na integriran sistem za upravljanje digitalnih identitet, celovito zaščito in varovanje identitete
3. Izdelava načrta za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
4. Vzpostavitev centralnega imenika na upravi Univerze in pilotna uporaba z izbrano aplikacijo
5. Sodelovanje pri pilotni postavitvi sistema in testiranje delovanja

V prvem obdobju izvajanja projekta se je projektna skupina iz Laboratorija za računalniške komunikacije na FRI v sodelovanju z rektoratom Univerze v Ljubljani ukvarjala predvsem z uvodnimi oziroma vzpostavitvenimi aktivnostmi, potrebnimi za uspešen zagon projekta. Prvi vsebinski sklop pa je bila izdelava analize problematike, primerjava sistemov za upravljanje digitalnih identitet in izbira najprimernejšega sistema za upravljanje digitalnih identitet glede na specifiko Univerze in na obstoječo tehnološko osnovo, ki že obstaja v informacijski službi Univerze v Ljubljani. Na podlagi vsega tega je bila med obravnavanimi sistemi izbrana Microsoftova platforma, kot središče sistema pa osrednji aktivni imenik, prek katerega katerega se bodo avtenticirali tako študentje kot tudi zaposleni.

V drugem obdobju izvajanja projekta Upravljanje z digitalnimi identitetami na Univerzi v Ljubljani je bila ključna aktivnost projektne skupine v sodelovanju z Rektoratom priprava načrta za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet.

Projektna skupina je najprej analizirala obstoječe stanje na UL, saj posamezne članice (fakultete,...) vodijo podatke o identitetah uporabnikov na heterogene načine, v različnih imeniških sistemih, ki so med seboj težko združljivi. Pri prehajanju med inštitucijami je zato zaposlenim in študentom dokazovanje identitete otežkočeno ali pa povezano z zapletenimi administrativnimi postopki. Ugotovljeno je bilo, da ima 13 članic lastne imenike. 6 je vključenih v t.i. gozd UNI-LJ, preostale pa imeniške storitve nimajo implementirane. Druga aktivnost v tem časovnem odbobju je bila zasnova arhitekture bodoče rešitve, ki bo sestavljena iz treh ključnih delov: osrednjega aktivnega imenika, sistema za sinhronizacijo podatkov o identitetah z zalednimi sistemi in sistema za upravljanje z digitalnimi potrdili.

Ključna aktivnost te faze projekta pa je bil razvoj načrta za uvedbo opisanega sistema. V njem so bile postavljene zahteve po ustrezni odzivnosti, visoki razpoložljivosti in odpornosti na napake, ovrednotene so bile infrastrukturne zahteve – računalniki ter ustrezna programska in strojna oprema,standardi poimenovanja in podobno. Načrt zagotavlja, da se bodo imeniški podatki pravilno replicirali po sistemu in bodo zato vedno na voljo uporabnikom. Prilagojen je omrežni topologiji in obstoječi komunikacijski infrastrukturi UL, zato zagotavlja tudi ustrezno odzivnost

[1] Potrebno je napisati vsebinsko raziskovalno poročilo, kjer mora biti na kratko predstavljen program dela z raziskovalno hipotezo in metodološko-teoretičen opis raziskovanja pri njenem preverjanju ali zavračanju vključno s pridobljenimi rezultati projekta.

in robustnost.

V tretjem obdobju smo pripravili strategijo prehoda na integriran sistem za upravljanje digitalnih identitet, ki vključuje tudi celovito zaščito in varovanje identitete. Strategija zajema naslednja področja:
a) Poimenovanje objektov v centralnem imeniku
b) Migracija digitalnih identitet zaposlenih iz obstoječih imenikov v nov centralni imenik
c) Ustvarjanje in upravljanje digitalnih identitet za študente UL
d) Ustvarjanje in upravljanje digitalnih identitet za zaposlene na UL
e) Preslikava in usklajevanje atributov med imenikom in zalednimi sistemi (Vpis, Kadrovska evidenca, E-študent,...)
f) Priporočila za razvoj aplikacij

Glavni aplikativni rezultat je bil dosežen v zadnjem obdobju v sodelovanju z zunanjimi izvajalci UL, in sicer vzpostavljen osrednji imenik Univerze, v katerem so podatki o vseh študentih in zaposlenih UL, ki samodejno skrbi za replikacijo podatkov po vseh lokacijah porazdeljene infrastrukture in ki se je v začetku pilotno uporabljal za avtentikacijo uporabnikov zalednih aplikacij, sedaj pa se z začetkom produkcijske uporabe nove študijske informatike UL tudi produkcijsko uporablja za avtentikacijo.

V času trajanja projekta smo torej dosegli zastavljene cilje oziroma mejnike: Opravljena je bila analiza in izbran najprimernejši sistem za upravljanje digitalnih identitet. Izdelan je bil načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet. Pripravljena je bila strategija prehoda na integriran sistem za upravljanje digitalnih identitet. Vzpostavljen je bil centralni imenik na upravi Univerze, delovanje pilotnega sistema je bilo pretestirano, celoten sistem je v produkcijski uporabi in za avtentikacijo ga že uporabljajo nove aplikacije, ki so prav tako že v produkcijski uporabi. Izkušnje s projekta so bile opisane v več člankih, nekateri so že objavljeni, zadnji pa je oddan v objavo.

3. Izkoriščanje dobljenih rezultatov:

3.1. Kakšen je potencialni pomen[2] rezultatov vašega raziskovalnega projekta za:

- ☐ a) odkritje novih znanstvenih spoznanj;
- ☒ b) izpopolnitev oziroma razširitev metodološkega instrumentarija;
- ☐ c) razvoj svojega temeljnega raziskovanja;
- ☐ d) razvoj drugih temeljnih znanosti;
- ☒ e) razvoj novih tehnologij in drugih razvojnih raziskav.

3.2. Označite s katerimi družbeno-ekonomskimi cilji (po metodologiji OECD-ja) sovpadajo rezultati vašega raziskovalnega projekta:

☐ a) razvoj kmetijstva, gozdarstva in ribolova - Vključuje RR, ki je v osnovi namenjen razvoju in podpori teh dejavnosti;

☐ b) pospeševanje industrijskega razvoja - vključuje RR, ki v osnovi podpira razvoj industrije, vključno s proizvodnjo, gradbeništvom, prodajo na debelo in drobno, restavracijami in hoteli, bančništvom, zavarovalnicami in drugimi gospodarskimi dejavnostmi;

☐ c) proizvodnja in racionalna izraba energije - vključuje RR-dejavnosti, ki so v funkciji dobave, proizvodnje, hranjenja in distribucije vseh oblik energije. V to skupino je treba vključiti tudi RR vodnih virov in nuklearne energije;

☐ d) razvoj infrastrukture - Ta skupina vključuje dve podskupini:

- transport in telekomunikacije - Vključen je RR, ki je usmerjen v izboljšavo in povečanje varnosti prometnih sistemov, vključno z varnostjo v prometu;
- prostorsko planiranje mest in podeželja - Vključen je RR, ki se nanaša na skupno načrtovanje mest in podeželja, boljše pogoje bivanja in izboljšave v okolju;

☐ e) nadzor in skrb za okolje - Vključuje RR, ki je usmerjen v ohranjevanje fizičnega okolja. Zajema onesnaževanje zraka, voda, zemlje in spodnjih slojev, onesnaženje zaradi hrupa, odlaganja trdnih odpadkov in sevanja. Razdeljen je v dve skupini:

☐ f) zdravstveno varstvo (z izjemo onesnaževanja) - Vključuje RR - programe, ki so usmerjeni v varstvo in izboljšanje človekovega zdravja;

☒ g) družbeni razvoj in storitve - Vključuje RR, ki se nanaša na družbene in kulturne probleme;

☒ h) splošni napredek znanja - Ta skupina zajema RR, ki prispeva k splošnemu napredku znanja in ga ne moremo pripisati določenim ciljem;

☐ i) obramba - Vključuje RR, ki se v osnovi izvaja v vojaške namene, ne glede na njegovo vsebino, ali na možnost posredne civilne uporabe. Vključuje tudi varstvo (obrambo) pred naravnimi nesrečami.

[2] Označite lahko več odgovorov.

3.3. Kateri so **neposredni rezultati** vašega raziskovalnega projekta glede na zgoraj označen potencialni pomen in razvojne cilje?

Neposredni rezultati:
- Metodologija za vzpostavitev sistema za upravljanje z digitalnimi identitetami v velikih in kompleksnih okoljih
- Primerno strukturiran okvir strategije za upravljanje z digitalnimi identitetami
- Višji nivo informacijskih storitev, ki jih UL nudi študentom in zaposlenim in omogočanje integracije univerzitetnih sistemov

3.4. Kakšni so lahko **dolgoročni rezultati** vašega raziskovalnega projekta glede na zgoraj označen potencialni pomen in razvojne cilje?

- Metodologija za vzpostavitev sistema za upravljanje z digitalnimi identitetami v velikih in kompleksnih okoljih se lahko aplicira v sorodnih projektih
- Z nadgrajevanjem in vključevanjem novih vsebin okvir strategije za upravljanje z digitalnimi identitetami lahko postane de facto standard na tem področju
- Urejen sistem za upravljanje z digitalnimi identitetami je osnoven pogoj za nadaljnji razvoj sodobnih informacijskih storitev Univerze v Ljubljani, zato tudi dolgoročno omogoča višji nivo informacijskih storitev in integracijo univerzitetnih sistemov.

3.5. Kje obstaja verjetnost, da bodo vaša znanstvena spoznanja deležna zaznavnega odziva?

☒ a) v domačih znanstvenih krogih;
☐ b) v mednarodnih znanstvenih krogih;
☒ c) pri domačih uporabnikih;
☐ d) pri mednarodnih uporabnikih.

3.6. Kdo (poleg sofinancerjev) že izraža interes po vaših spoznanjih oziroma rezultatih?

Fakulteta za elektrotehniko in računarstvo iz Zagreba je vodjo projekta povabila na vabljeno predavanje s predstavitvijo rezultatov projekta. Predavanje bo 28. 4. 2009 v Zagrebu.

3.7. Število diplomantov, magistrov in doktorjev, ki so zaključili študij z vključenostjo v raziskovalni projekt?

2 diplomanta zaključila; 1 magistrant zaključuje.

4. Sodelovanje z tujimi partnerji:

4.1. Navedite število in obliko formalnega raziskovalnega sodelovanja s tujimi raziskovalnimi inštitucijami.

V okviru projekta ni bilo formalnega raziskovalnega sodelovanja s tujimi raziskovalnimi institucijami.

4.2. Kakšni so rezultati tovrstnega sodelovanja?

5. Bibliografski rezultati[3] :

Za vodjo projekta in ostale raziskovalce v projektni skupini priložite bibliografske izpise za obdobje zadnjih treh let iz COBISS-a) oz. za medicinske vede iz Inštituta za biomedicinsko informatiko. Na bibliografskih izpisih označite tista dela, ki so nastala v okviru pričujočega projekta.

6. Druge reference[4] vodje projekta in ostalih raziskovalcev, ki izhajajo iz raziskovalnega projekta:

Mojca Ciglarič: Building an Identity Management Strategy. Oddan članek v revijo European Journal of Information Systems, Palgrave McMillan (v recenziji). Mojca Ciglarič: Digital Identity Management Strategy. Predavanje na povabilo IEEE ComSoc in Zavoda za telekomunikacije FER-a. Zagreb 28.4. 2009.

[3] Bibliografijo raziskovalcev si lahko natisnete sami iz spletne strani:http:/www.izum.si/

[4] Navedite tudi druge raziskovalne rezultate iz obdobja financiranja vašega projekta, ki niso zajeti v bibliografske izpise, zlasti pa tiste, ki se nanašajo na prenos znanja in tehnologije.
Navedite tudi podatke o vseh javnih in drugih predstavitvah projekta in njegovih rezultatov vključno s predstavitvami, ki so bile organizirane izključno za naročnika/naročnike projekta.

Strategija upravljanja z digitalnimi identitetami

PRILOGE:

1) BIBLIOGRAFIJA vodje projekta M. Ciglarič (Ker so v vseh objavljenih prispevkih soavtorji vsi člani projektne skupine, ločenih bibliografij ostalih članov ne prilagamo – v njih ni nobenih dodatnih prispevkov z rezultati projekta).
2) Dokument: Strategija upravljanja z digitalnimi identitetami Univerze v Ljubljani
3) Dokument: Načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
4) Članek (DSI): Uvajanje enotnega upravljanja z digitalnimi identitetami na Univerzi v Ljubljani
5) Članek (Inf. družba): Strategija upravljanja z digitalnimi identitetami
6) Članek (v recenziji): Building an Identity Management Strategy

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Strategija upravljanja z digitalnimi identitetami na Univerzi v Ljubljani

Dokument	Strategija upravljanja z digitalnimi identitetami na Univerzi v Ljubljani
Avtorji	Mojca Ciglarič, Andrej Krevl, Matjaž Pančur
Različica	1.0
Datum nastanka	25. 4. 2008
Datum zadnje spremembe	25. 4. 2008

Kazalo

1. Uvod

Celostna strategija upravljanja z digitalnimi identitetami v tako veliki organizaciji, kot je Univerza v Ljubljani, mora oziroma naj bi služila kot vodilo za izvedbo posameznih namenskihprojektov ali faz projektov, za katere v organizaciji obstaja imperativ za zagotavljanje s strategijo skladnega obravnavanja identitete. Končni cilj je, da bi bili s strategijo skladni vsi posamezni deli.Strategijo upravljanja z digitalnimi identitetami vedno sestavlja več vsebinsko zaokroženih sestavnih delov, tipični so upravljanje gesel, nadzor dostopa, osrednji imenik in podobno.

Splošni cilji upravljanja z digitalnimi identitetami UL, ki jih zasleduje tudi pričujoča Strategija upravljanja z digitalnimi identitetami, so naslednji:

1. **Udobje in boljša storitev za uporabnika**: to dvoje se uresničuje s pomočjo zmanjšanja števila različnih identitet uporabnika (različna uporabniška imena in gesla za različne aplikacije in sisteme) – v končni fazi se uresniči enkratno prijavljanje z eno samo identiteto (single sign-on). Ena sama identiteta pa pomeni tudi eno samo mesto za vzdrževanje podatkov o dostopu v različne sisteme in o kontaktnih ter drugih podatkih uporabnika. Za uresničenje le tega je potrebna ustrezna povezava s končnimi (zalednimi) aplikacijami in vmesnik za končnega uporabnika, če mu dovolimo, da tudi sam vnaša in spreminja svoje podatke.

2. **Podpora e-poslovanju:** zaledni sistemi in aplikacije lahko izvajajo avtorizacijo in avtentikacijo uporabnikov, uporabniki pa lahko (celo znotraj ene transakcije) dostopajo do podatkov in storitev, ki jih sicer nudijo različni zaledni sistemi in aplikacije.

3. **Osrednji imenik:** imenik je središčna točka vsakega sistema za upravljanje z digitalnimi identitetami in predstavlja povezavo s podatki v zvezi z identitetami v zalednih sistemih. S svojimi podatki ponazarja tudi posnetek organizacijske strukture, obenem pa zaradi poenotenega upravljanja z identiteto na enem mestu znižuje stroške vodenja in povezovanja imenikov.

4. **Organizacijska struktura**: z ustreznim dodeljevanjem vlog uporabnikom sistema se ustvarja posnetek organizacijske strukture in konsistentno dodeljevanje pravic in omejitev uporabnikom z enakimi vlogami. Uporabnike se lahko obravnava bodisi skupinsko bodisi individualno, s tem se tudi olajšuje delo administratorjem.

5. **Delovni tokovi**: vzpostavljen sistem upravljanja z digitalnimi identitetami omogoča informacijsko podporo izvajanja delovnih tokov poslovnega procesa (tudi prek več zalednih sistemov in aplikacij), v katerih uporabniki sodelujejo na podlagi svojih dodeljenih vlog. Okolje za izvajanje podatkovnih tokov ali upravljanje poslovnih procesov je lahko ločeno od sistema za upravljanje digitalnih identitet – povezano je le toliko kot vsak zaledni sistem.

6. **Zagotavljanje in nadzor dostopa do virov** (provisioning): Uporabnik avtomatsko dobi dostop do tistih virov, aplikacij in sistemov, ki pripadajo njemu dodeljenim vlogam. Obenem ima onemogočen dostop do tistih virov, aplikacij in podsistemov, ki njemu dodeljenim vlogam ne pripadajo. V primeru spremembe uporabnikovega statusa (npr. premestitev na drugo delovno mesto ali odpoved) se s preprosto spremembo – dodajanjem ali odvzemom ustrezne vloge – zagotovi tudi dostop do ustreznih virov.

7. **Varnost in zasebnost:** Zmanjšaaliizniči se potreba po pomnjenju, varnem hranjenju ali zapisovanju številnih uporabniških imen in gesel za dostop do različnih sistemov. Prav tako se zmanjša ali izniči potreba po skupinskih geslih, ki so še zlasti varnostno problematična.

2. Sedanje stanje in pričakovane težave

Vsi študentje, učitelji, asistenti, raziskovalci, pa tudi nekdanji študentje, diplomanti, magistranti in doktoranti, upokojeni člani morajo imeti možnost preprostega, a vendar varnega dostopa do virov univerzitetnega sistema in do njegovih storitev s kateregakoli konca interneta. Ta zahteva pogojuje izgradnjo odprte, a varne informacijske infrastructure, učinkovitih in razširljivih procesov upravljanja dostopa do virov, in uveljavljanje striktnih pravil in zahtev glede dostopa do univerzitetnih informacijskih virov in storitev.

Izzivi, s katerimi se bo pri tem srečala UL, so številni. Iz do sedaj napisanega je jasno, da so sistemi za upravljanje z identitetami veliki in kompleksni. Čeprav bi vzpostavljen sistem Univerza potrebovala že danes, se bo vzpostavljal v daljšem časovnem obdobju kot zaporedje več ločenih informacijskih projektov z manjšimi, a jasno določenimi cilji (na primer projekt zagotavljanja enotnih elektronskih naslovov za vse študente, projekt vzpostavitve univerzitetne certifikatne agencije, ...). Vsi ti projekti bodo morali upoštevati enotno strategijo in enotne varnostne politike, ki pa žal še niso napisane. Zagotavljati bodo morali razširljivost na več desetin tisočev uporabnikov in nuditi visoko stopnjo razpoložljivosti (zaželjen je ciljni razred "pet devetk", torej 99.999% časa sistem deluje), kar za seboj potegne tudi redundančno zasnovano infrastrukturo in primerno organizacijo dela v informacijski službi Univerze.

Ker se v sistemu za upravljanje z digitalnimi identitetami hranijo tudi osebni podatki, je potrebno pri vzpostavljanju upoštevati Zakon o varovanju osebnih podatkov in v skladu z njim še bolj pozorno zagotoviti varno hranjenje podatkov in onemogočanje nepooblaščenega dostopa.

Možno je, da bo Univerza v bodočnosti omogočala tudi povezovanje z informacijskimi sistemi drugih organizacij in inštitucij (na primer prijava na razpise ARRS), mora sistem za upravljanje z digitalnimi identitetami omogočati tudi združevanje (federation) identifikacijskih podatkov iz različnih sistemov za upravljanje z digitalnimi identitetami po principih danes splošno sprejetih /standardnih tehnologij s tega področja.

3. Predlog strategije za upravljanje z digitalnimi identitetami

3.1. Ena identiteta za eno osebo

Vsak zaposleni in vsak študent Univerze v Ljubljani naj bi imel eno samo elektronsko identiteto, ki naj bi jo v zadnji fazi uporabljal za dostop do vseh informacijskih sistemov in storitev, do katerih je upravičen dostopati.

S pomočjo ene enotne identitete bo olajšano tudi prehajanje študentov in učiteljev med članicami, ki ga poudarja bolonjski proces, saj bodo študentje in profesorji do informacijskih virov na različnih članicah UL dostopali z eno samo identiteto.

3.2. Ustvarjanje nove digitalne identitete

Študentje prejmejo svojo digitalno identiteto ob vpisu na fakulteto. Za vsakega študenta se ustvari uporabniško ime in naključno začetno geslo. Če se študent strinja s pogoji uporabe informacijskih storitev UL, lahko s pomočjo teh podatkov aktivira (omogoči) svoje uporabniško ime, si nastavi svoje geslo in (če to želi) dopolni podatke v svojem profilu. Ob prvi aktivaciji digitalne identitete so uporabniške pravice minimalne. Seveda se potrebe za dostop do informacijskih virov UL v toku študijskega procesa spreminjajo, zato omogoča sistem za upravljanje digitalnih identitet dodeljevanje in odvzemanje vlog uporabnikom. Skrbniki sistema na članicah lahko dodeljujejo vloge za dostop do računalniških učilnic, datotečnih virov, tiskalnikov, ipd. Na drugi strani pa se tudi nabor informacijskih storitev, ki jih nudi informacijska služba UL, povečuje, s tem pa se povečuje tudi število vlog, ki pripadajo posameznem študentu. Zato imajo tudi skrbniki sistema na UL možnost dodajanja in odvzemanja vlog študentom. Omogočeno je tudi dodajanje začasnih vlog, kot je na primer sodelovanje na različnih projektih Ob zaključku študija ostane uporabniško ime aktivno, le da se ga uvrsti v program Alumni, odvzame pa se večina vlog, ki omogočajo dostop do informacijskih virov UL.

Zaposlenim se ustvari digitalna identiteta takoj ob nastopu dela. Sistem za upravljanje digitalnih identitet nenehno pregleduje spremembe v kadrovskih evidencah in na podlagi novega zapisa v kadrovski evidenci ustvari novo digitalno identiteto za zaposlenega. Kljub temu, da zaposleni nastopajo v drugačnih vlogah kot

študentje, pa je upravljanje z vlogami rešeno na zelo podoben način. Vloge, ki omejujejo dostop do virov na posameznih članicah upravljajo skrbniki na članicah, globalne vloge za dostop do informacijskih virov UL pa upravljajo skrbniki v informacijski službi UL.

O digitalni identiteti smo do sedaj govorili kot o kombinaciji uporabniškega imena in gesla, vendar pa sistem za upravljanje digitalnih identitet omogoča in tudi predvideva tudi močnejše načine avtentikacije uporabnikov. Kot eno izmed naslednjih faz projekta omenimo uvajanje digitalnih potrdil za vse uporabnike UL.

3.3. Minimalne pravice, ki jih ima vsaka digitalna identiteta

Minimalne pravice digitalnih identitet na UL se razlikujejo glede na vlogo posameznika. Pri študentih obsega minimalen nabor pravic:

- dostop do aplikacije e-Študent,
- uporaba Info točk na članicah,
- dostop do brezžičnega omrežja Eduroam,
- dostop do nekaterih knjižničnih gradiv,
- elektronski naslov v domeni student.uni-lj.si.

Za zaposlene pa obsega minimalen nabor pravic:

- dostop do brezžičnega omrežja Eduroam,
- dostop do nekaterih knjižničnih gradiv,
- elektronski naslov v domeni uni-lj.si ali clanica.uni-lj.si.

3.4. Kreiranje digitalne identitete z več pravicami oziroma dodajanje pravic

Nove vloge in s tem pravice za dostop do informacijskih virov se dodajajo v skladu s potrebami pedagoškega procesa ali delovnimi nalogami posameznika. Nove vloge zaposlenega se lahko dodelijo na podlagi spremembe delovnih nalog, zaradi sodelovanja na projektu, zaradi dodatnih pedagoških obremenitev na drugih članicah, ipd. Vloge študentov se lahko spreminjajo ob vpisu v knjižnico, ob pridobitvi novega statusa (vpis v nov študijski program, zaključek študija), ob vključevanju v različne projektne skupine, ipd. Za dodeljevanje vlog, ki vključujejo pravice dostopa do lokalne infrastrukture na članici skrbijo sistemski skrbniki na članicah. Za dodeljevanje vlog, ki vključujejo pravice dostopa do univerzitetnih

informacijskih virov, skrbi informacijska služba UL. Sistem za upravljanje digitalnih identitet naj omogoča tudi določeno avtomatiko dodeljevanja vlog na podlagi sprememb v podatkovnih bazah študijske informatike in kadrovske evidence. Seveda pa ne moremo pričakovati popolnega avtomatizma, saj je dodeljevanje vlog na npr. posamezne projekte zaradi značilnosti posameznih zalednih sistemov skoraj nemogoče avtomatizirati.

3.5. Uporabniške skupine ali grupe (tudi varnostne skupine – security groups)

Uporabniške skupine pogosto olajšajo sistemsko administracijo in omogočajo preprosto zagotavljanje konsistentnosti pravic in omejitev. Pri ustvarjanju uporabniških skupin sta dovoljena dva pristopa.

Prvi pristop predstavlja ustvarjanje skupine tako, da se vsem članom dodeli enake vloge. Drugi pristop pa predstavlja ustvarjenje skupinskega objekta (na primer e-poštnega naslova) in nato poljubno dodajanje uporabnikov v to skupino. V vsakem primeru za ustvarjanje in vzdrževanje skupin potrebujemo ustrezna administratorska orodja.

V okviru informacijskega sistema UL med vlogami in skupinami ne ločujemo. Pravice, povezane s posamezno vlogo, so pravice, ki pripadajo določeni varnostni skupini v osrednjem imeniku UL. Poleg globalnih skupin, ki veljajo na nivoju celotnega imenika in se začnejo s predpono *UL_*, ima vsaka članica možnost, da ustvari lastne varnostne skupine, ki omogočajo dodeljevanje pravic do različnih virov. Skupine članic se začnejo s predpono *CLANICA_* in nadaljujejo z imenom skupine.

Med globalnimi vlogami so tudi vloge, ki omogočajo aplikacijam avtentikacijo in avtorizacijo uporabnikov. Te vloge so vedno poimenovane v oblikiUL_ImeAplikacije _ImeVloge. Za včlanjevanje uporabnikov v te vloge lahko skrbi sistem za upravljanje digitalnih identitet ali pa informacijska služba UL.

3.6. Elektronski naslovi

Kot za digitalne identitete tudi za elektronske naslove velja, da naj bi imel vsak zaposleni in vsak študent svoj elektronski naslov v domeni Univerze. Elektronski naslov pa se ne sme uporabljati za dokazovanje identitete! To naj bo le eden od podatkov v profilu uporabnika. Naslove se lahko razvršča tudi v skupine, prav tako lahko obstajajo skupinski naslovi (distribucijski seznami) za zaposlene (asistenti,

učitelji, raziskovalci...) in za študente (študenti določenega študije, letnika, smeri, predmeta, ...).

3.7. Prijava v aplikacije in dostop do storitev, ki jih nudi UL

Zaželeni način prijave v zadnji fazi uvajanja sistema digitalnih identitet naj bi bila enotna prijava (Single Sign-On oz. SSO). To za uporabnika pomeni, da se najprej prijaviv spletni portal, nato pa se mu v druge aplikacije ni potrebno ponovno prijavljati, saj je že avtenticiran in ga sistem pozna.. Dokler to ni tehnično omogočeno (tudi zaradi same tehnologije obstoječih aplikacij), je sprejemljiva neposredna prijava v ciljno aplikacijo, ki pa naj za avtentikacijo uporablja podatke iz osrednjega imeniškega sistema (princip "campus-wide login"). Pri tem principu uporabnik še vedno uporablja zgolj eno uporabniško ime in geslo za dostop do različnih storitev, vendar pa ga mora vnašati na različnih mestih (v različnih aplikacijah).

3.8. Preprečevanje zlorab

Z uvedbo enotnih identitet in centralnega imenika se povečuje tudi varnostno tveganje ob kraji posameznikove identitete, saj ena identiteta omogoča dostop do vseh informacijskih virov UL. Poskrbeti je potrebno, da identitete ni možno zlorabiti, torej ni možno (ali pa je zelo težko) uporabiti identiteto nekoga drugega. Zloraba je lahko kritična na primer pri izpitih, manj kritična pa v primeru, ko lastnik identitete to prostovoljno "posodi" za dostop do svojih virov. Uporabnike je potrebno izobraziti, da imatudi »neškodljivo posojanje« identitet, lahko za posledico resno ogrožanje posameznikove varnosti.

4. Zaključek

V tem razdelku povzemamo do sedaj napisano v obliki kratkega, zgoščenega seznama ciljev, ki jih naj dosega sistem za upravljanje z digitalnimi identitetami, ko bo izgrajen in vpeljan do konca.

1. Omogočati varen in zanesljiv dostop do informacijskih virov in storitev
2. Zagotoviti varnost in zaupnost podatkov.
3. Zmanjšati stroške oziroma napore, potrebne za vzdrževanje sistema in obenem zvišati učinkovitost.
4. Omogočiti skrbnikom preprosto upravljanje uporabniških podatkov in pravic dostopa.
5. Preprečevati neprimerno rabo in nepooblaščen dostop do virov.
6. Omogočati preprosto in učinkovito pomoč in uporabniško podporo.
7. Uveljavljati ustrezne organizacijske politike dostopa do informacijskih virov in storitev.
8. Omogočati avtomatizacijo poslovnih procesov in usmerjanje s tem povezanih podatkov preko centralnega "preklopnika" ali organizacijskega storitvenega vodila.
9. Izničiti potrebo po vnosih istih (osebnih) podatkov v več različnih sistemov.
10. Podpora združevanju sistemov.

Da bo sistem za upravljanje z digitalnimi identitetami lahko zasledoval navedene cilje, bo moral implementirati naslednjo funkcionalnost:

1. Osrednji aktivni imenik s podatki o posameznikih, vlogah in dostopih.
2. Avtentikacija ali potrjevanje (dokazovanje) identitete uporabnika (na primer z geslom; danes je bolj zaželena večkratna avtentikacija).
3. Avtorizacija: Določanje dovoljenj za dostop. Individualna, na temelju vloge - skupinska, ali anonimna (prek drugega sistema, ki mu zaupam).

4. Eno uporabniško ime in geslo ter ena prijava za dostop v vse povezane sisteme. Omogočanje uporabniku, da sam vzdržuje svoje podatke (self-provisioning).
5. Omogočanje prenosa pravic in uporabe podatkov IM sistema v aplikacijah.
6. Preprosta in vsaj deloma razpršena administracija.
7. Prožno določanje pravic.
8. Ustvarjanje in upravljanje vlog.

In končno, lahko na podlagi izkušenj opredelimo tudi pričakovane koristi in prednosti, ki jih bo prinesel dobro uveden sistem upravljanja z digitalnimi identitetami - nekatere so lahko opazne in celo merljive, druge pa lahko bolj začutimo kot ovrednotimo, vendar pa niso zato nič manj pomembne.

1. Zmanjšana količina dela na podpori uporabnikov: manj menjave gesel, manj administriranja uporabniških računov, krajši čas za odprtje novega uporabniškega računa, avtomatiziran prenos podatkov med sistemi (npr. avtomatska ulinitev računa uporabniku, ki je dal odpoved).
2. Boljši nadzor in sledenje uporabe virov, aplikacij in storitev.
3. Manj varnostnih incidentov.
4. Centralizirana administracija sistema za opaovanje in nadzor.
5. Manj neaktivnih računov.

5. DODATEK: Konkretni podatki o sedanjem stanju informacijske infrastrukture, imeniških sistemov in upravljanja z identitetami na UL kot dopolnitev splošne strategije upravljanja z digitalnimi identitetami na UL

Zaradi konsistentnosti polnjenja in uporabe sistema za upravljanje digitalnih identitet je potrebno za vsak vsebinski sklop podatkov v zvezi z identitetami odgovoriti na nekaj ključnih vprašanj:

- Kaj je avtoritativni vir podatkov za ta sklop?
- Kako poteka sinhronizacija z osrednjim imenikom in zalednimi sistemi?
- Kaj se zgodi ob spremembi podatka v avtoritativnem viru?

Nekaj smernic nudi na primer Microsoft na naslovu http://www.microsoft.com /windowsserver2003/technologies/idm/ilm.mspx

Na UL predstavljajo glavne vire podatkov naslednji informacijski podsistemi:

- Kadrovska evidenca
- Vpis (visokošolska prijavno - informacijska služba)
- Študijska informatika (E- študent)
- Aplikacija za projektno vodenje (4PM)
- Spletni portal, kjer uporabniki lahko sami vnašajo in spreminjajo podatke v zvezi s svojo digitalno identiteto (self-provisioning portal)

5.1. Upravljanje digitalnih identitet za študente

V nadaljevanju je opisan trentuno predvideni in predpisani postopek za dodeljevanje digitalnih identitet študentom in za njihovo nadaljnje upravljanje.

1. Vpisna služba pripravi spisek kandidatov v obliki primerni za nadaljnjo obdelavo v okviru povezovalnega modula Esperanto (datoteka v formatu CSV).

2. Esperanto generira **unikatna** uporabniška imena (tudi UPN v obliki ime.priimek@student.uni-lj.si) in začetna gesla ter jih doda v spisek kandidatov.

3. Dopolnjen spisek kandidatov se uvozi:

    a. V aplikacijo E–študent 3G.
    b. V MIIS strežnik, ki podatke o kandidatih replicira v ActiveDirectory (student.uni-lj.si). Atribut eduPersonAffiliation se nastavi na »candidate« (začasni atribut).

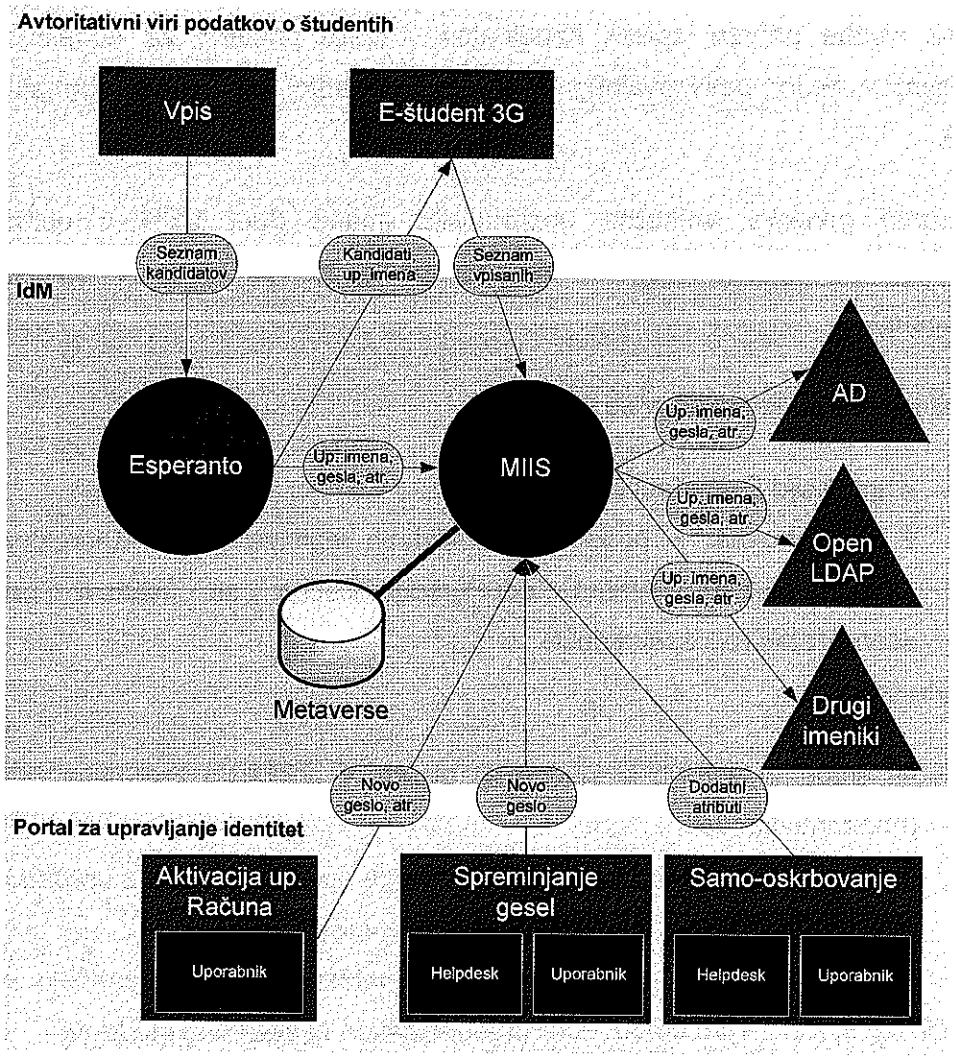
4. Vpis študenta:

    a. Ali študenta vpišejo v študentski pisarni v aplikacijo E-študent 3G (papirnati obrazci).
    b. Ali pa se študent s pomočjo interaktivnega spletnega vpisa z uporabo uporabniškega imena in začetnega gesla vpiše sam.

5. Ob vnaprej določenih časovnih intervalih se vpisani študenti prenašajo v strežnik MIIS, kjer se jim atribut eduPersonAffiliation nastavi na »student«.

6. Vpisani študent (eduPersonAffiliation = student) lahko s pomočjo spletnega portala za upravljanje identitet aktivira vse ostale informacijske storitve (Eduroam, E-mail, ...), ki mu jih nudi Univerza v Ljubljani. Aktivacija poteka tako, da se mora študent za vklop posamezne storitve eksplicitno strinjati s pogoji uporabe te storitve (TOU = Terms of Use). Ko se s pogoji uporabe strinja, se v strežniku MIIS nastavijo ustrezni atributi, njegova identiteta pa se sinhronizira v ustrezne imenike (če je to potrebno). Če študentov eduPersonAffiliation ni enak »student«, se študent v spletni portal ne more prijaviti.

Opisani postopek grafično prikazuje slika 1.



Slika 1: Polnjenje imenika 2008

5.2. Spreminjanje gesel in upravljanje digitalne identitete

Študent spreminja svoje geslo izključno preko spletnega portala za upravljanje identitet.V vseh drugih aplikacijah, ki za avtentikacijo in avtorizacijo uporabljajo Active Directory, mora biti spreminjanje gesla onemogočeno. Spreminjanje gesla mora biti onemogočeno tudi navseh računalnikih, ki so dostopni študentom. To je potrebno zaradi sinhronizacije gesla na vse sisteme.

5.2.1. Zamenjava gesla

Študent svoje geslo zamenja izključno prek portala za upravljanje identitet. Za menjavo gesla mora najprej vnesti svoje staro geslo, nato pa dvakrat novo geslo. Sinhronizacija gesel v druge sisteme poteka v realnem času.

5.2.2. Pozabljena gesla

5.2.3. Ponastavitev gesla na začetno geslo

Ponastavitev pozabljenega gesla lahko študent opravi s telefonskim klicem naslužbo pomoči - helpdesk UL. Pred zahtevo za ponastavitev se mora ustrezno identificirati (ime, priimek, vpisna številka,...). Operater s pomočjo spletnega portala za upravljanje digitalnih identitet ponastavi geslo na začetno vrednost.

5.2.4. Ponastavitev gesla

Če študent izgubi tudi začetno geslo, lahko sproži postopek ponastavitve gesla v referatu članice,na katero je vpisan. V referatu se mora identificirati z ustreznim dokumentom, opremljenim s sliko.Uslužbenec referata s pomočjo spletnega portala za upravljanje digitalnih identitet ponastavi geslo na novo vrednost.

5.3. Upravljanje digitalnih identitet zaposlenih:

5.3.1. Vir podatkov

Avtoritativen vir podatkov za podatke o zaposlenih je vsekakor aplikacija »Kadrovska evidenca« (KE), saj le-ta združuje vse podatke o posamezniku.Trenutno imamo pri tem težavo, saj KE ne pozna posameznikove digitalne identitete iz centralnega imenika (AD).Ker želimo kljub temu povezati digitalne identitete zaposlenih z njihovimi podatki v KE, je potrebno shemo atributov v AD razširiti z enolično šifro zaposlenega (IC) iz KE. Predlagamo širitev sheme AD z atributom:

siEduPersonUlHrUid

Atribut lahko vsebuje do 13 alfanumeričnih znakov.

5.3.2. Drugi viri

Med druge vire podatkov lahko trenutno umestimo tudi obstoječe imenike AD po članicah.Vendar pa ti viri niso avtoritativni.Upoštevati jih moramo le kot izvor identitet, ki jih je potrebno povezati s podatki iz kadrovskih evidenc.

Predlagamo naslednji postopek za dodajanje atributa siEduPersonUlHrUid v AD:

Iz KE se pripravi seznam zaposlenih z naslednjimi atributi:

- ime,

- priimek,
- IC.

Posameznika v imeniku poiščemo z njegovim imenom in priimkom. Vnesemo vrednost IC v siEduPersonUlHrUid. Če so vnosi za določeno ime in priimek podvojeni, se takšne vnose posebej označi na seznamu iz KE. Informacijska služba na članici poskrbi za reševanje podvojenih imen/priimkov, označenih na prejšnjem koraku.

5.3.3. Atributi v AD

Atributi, ki jih za zaposlenega hranimo v centralnem imeniku in po katerih lahko zaposleni na UL iščejo druge zaposlene, so:

- ime (KE),
- priimek (KE),
- službena telefonska številka (stvar self-provisioning portala),
- članica (KE),
- elektronska pošta (v QT je vnesena osebna e-pošta, ne pa univerzitetna, tudi stvar self-provisioning portala),
- IC (to je skriti atribut => ne prikazujemo ga pri iskanju).

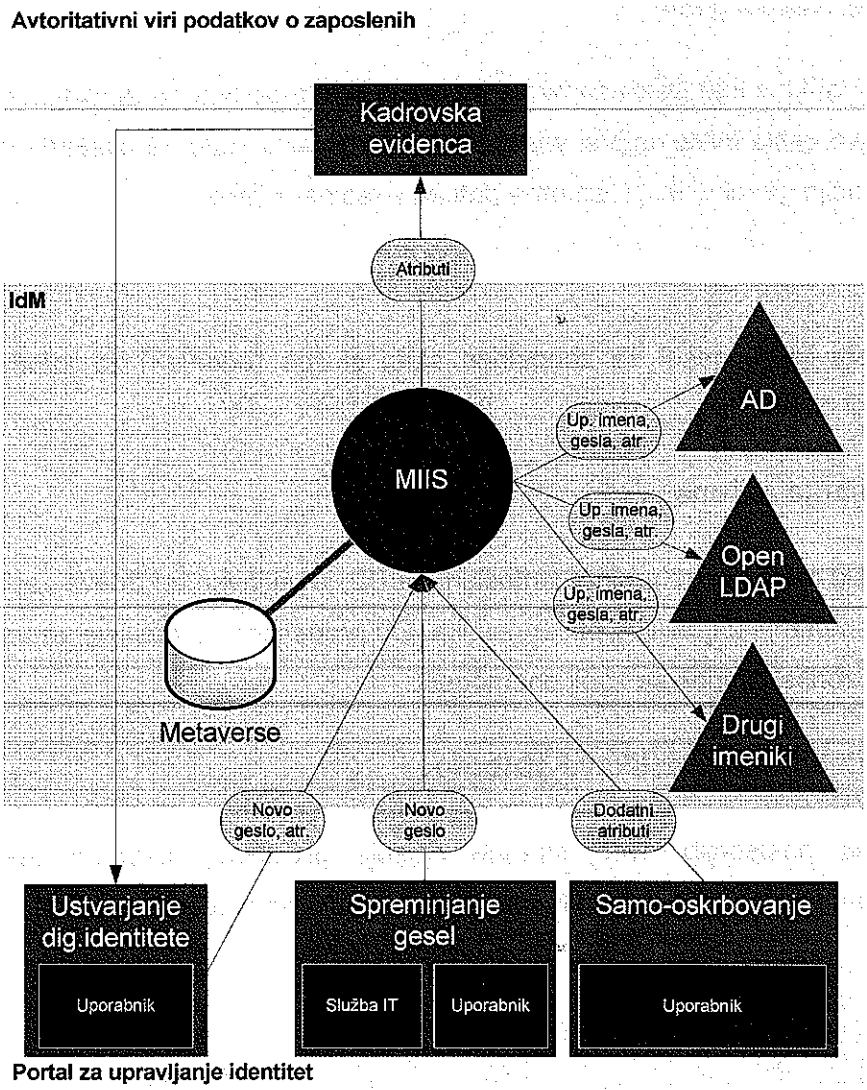
5.4. Ustvarjanje novega uporabnika

Kadrovska služba skupaj z vnosom novega zaposlenca v aplikacijo KE s pomočjo obrazca na portalu za upravljanje digitalnih identitet ustvari tudi njegov uporabniški račun. V kolikor je za posameznika potrebno dodeliti tudi nestandardne varnostne nastavitve se istočasno v službo za informatiko preda vloga za dodelitev posebnih privilegijev.

Vnesti je potrebno tudi podatke o veljavnosti, torej od kdaj do kdaj je digitalna identiteta veljavna (na primer, če ima oseba sklenjeno pogodbo s krajšim rokom veljavnosti).

5.4.1. Usklajevanje identitet

Usklajevanje identitet je grafično prikazano na sliki 2 spodaj.



Slika 2: Usklajevanje identitet zaposlenih

5.5. Spreminjanje gesel in upravljanje digitalne identitete

Zaposleni spreminjajo svoje geslo izključno preko spletnega portala za upravljanje identitet.V vseh drugih aplikacijah, ki za avtentikacijo in avtorizacijo uporabljajo Active Directory mora biti spreminjanje gesla onemogočeno. Spreminjanje gesla mora biti onemogočeno tudi na računalnikih, ki jih zaposleni uporabljajo pri vsakdanjem delu. Takšen postopek je potreben za procese sinhronizacije gesel na vse sisteme.

5.5.1. Zamenjava gesla

Zaposleni lahko svoje geslo zamenja izključno preko portala za upravljanje identitet. Za menjavo gesla mora najprej vnesti svoje staro geslo, nato pa dvakrat novo geslo. Sinhronizacija gesel v druge sisteme poteka v realnem času.

5.5.2. Pozabljena gesla

Za ponastavljanje gesel za zaposlene skrbi služba (oddelek) za informatiko na posamezni članici.

5.6. Trajanje računa

Uporabniški račun, ki ga prejme zaposleni na UL, je veljaven od dneva zaposlitve do dneva prenehanja zaposlitve posameznika. Ob prenehanju zaposlitve se uporabniški račun ne izbriše, ampak se zgolj onemogoči.

5.7. Medsebojne preslikave atributov

Tabela na naslednjih dveh straneh opisuje preslikavo oziroma medsebojne odvisnosti atributov prek različnih imeniških sistemov in zalednih aplikacij Univerze v Ljubljani.

Vpis	E-študent 3G	AD	OpenLDAP	MIIS Metaverse	Portal za upravljanje digitalnih identitet	Študentski e-mail (outsourcing)	Primer	Opis polja
userPrincipalName	?	userPrincipalName	eduPersonPrincipalName	eduPersonPrincipalName	Vse se hrani v AD	eduPersonPrincipalName	janez.novak@student.uni-lj.si	Uporabniško ime (UPN)
sAMAccountName		sAMAccountName	uid	uid			novakja	Uporabniško ime (pre Win2K)
IME	ime	givenName	givenName	givenName			Janez	Uradno osebno ime
PRIIMEK	priimek	sn	sn	sn		Sn	Novak	Priimek (vsi priimki), kot je naveden v uradnih evidencah
IME + PRIIMEK		cn	cn	cn		Cn	Janez Novak	Polno ime in priimek uporabnika, kot je navedeno v uradnih evidencah
IME + PRIIMEK		displayName	displayName	displayName			Janez Novak	Ime osebe, ki je uporabi oz. Kot ga navede uporabnik sam
PRIIMEK			schacSn1	schacSn1			Novak	Prvi priimek
PRIIMEK			schacSn2	schacSn2				Drugi priimek (če ima oseba le en priimek => prazno)
NASLOV	naslov							
POSTA	posta		postalCode	postalCode			SI-1000	Poštna številka z dvočrkovno predpono države
NASLOV + POSTA			postalAddress	postalAddress			Nekje 10$SI-1000 Ljubljana$Slovenia	Naslov stalnega bivališča
	Zacasno Bivalisce		registeredAddress	registeredAddress			Nekje 10$SI-1000 Ljubljana$Slovenia	Naslov začasnega prebivališča
userPrincipalName		mail	mail	mail			janez.novak@student.uni-lj.si	E-poštni naslov
eduPersonAffiliation		eduPersonAffiliation	eduPersonAffiliation	eduPersonAffiliation			alumni	Status osebe
eduPersonPrimaryAffiliation		eduPersonPrimaryAffiliation	eduPersonPrimaryAffiliation	eduPersonPrimaryAffiliation			teacher	Priamrni status osebe
spol	spol		schacGender	schacGender			2	Uradni spol osebe
emso	emso		schacDateOfBirth	schacDateOfBirth			19800303	Datum rojstva
emso			schacPersonalUniqueID	schacPersonalUniqueID			0303980500224	Enotna matična številka občana
	krajRojstva		schacPlaceOfBirth	schacPlaceOfBirth			Kočevje, Slovenia	Kraj in država rojstva
	drzavljanstvo		schacCountryOfCitizenship	schacCountryOfCitizenship			si	Državljanstvo - 2 črkovna ISO oznaka države

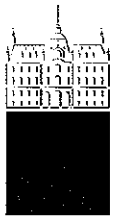
	naziv		schacPersonalTitle	schacPersonalTitle			dr.	Naziv
zavod	zavod	company	schacHomeOrganization	schacHomeOrganization			uni-lj.si	Registrirano DNS ime organizacije
	tipZavoda		schacHomeOrganizationType	schacHomeOrganizationType			urn:arnes.si:homeOrgType:fakulteta	Tip organizacije
	vpisnaStevilka		schacPersonalUniqueCode	schacPersonalUniqueCode			urn:arnes.si:personalPublicUniqueCode:vpisna številka:63775426	Študentova vpisna številka
		objectGUID	schacUUID	schacUUID			15afa00-13887-d468a687	Enoličen ID zapisa
	vpisanDo	accountExpires	schacExpiryDate	schacExpiryDate			200710302359592	Datum poteka veljavnosti (vključno)
		ulEduPersonEmailTOU					1	Atribut določa ali ima študent vključeno storitev elektronska pošta (Zf: 0/1)
		ulEduPersonEduroamTOU					1	Atribut določa ali ima študent vključeno storitev Eduroam (Zf: 0/1)
	clanica	company	o	o			Fakulteta za računalništvo in informatiko	Polno ime organizacije
	program	ulEduPersonProgram	ulEduPersonProgram	ulEduPersonProgram			Univerzitetni	Program v katerega je vpisan študent
	smer	ulEduPersonSpecialisation	ulEduPersonSpecialisation	ulEduPersonSpecialisation			Informatika	Smer v katero je vpisan študent
	letnik	ulEduPersonYear	ulEduPersonYear	ulEduPersonYear			1	Letnik v katerega je trenutno vpisan študent
userPassword		userPassword	userPassword			userPassword	mmjsmfjg	Uporabnikovo geslo (edini atribut, ki se sinhronizira v realnem času)

Izvor atributa

Avtoritativen vir atributa (če ni označen, potem je enak izvoru)

Izpeljani atribut

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*



Načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet

Dokument	Načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
Projektna skupina	M. Ladava, P. Zdovc, A. Jagodic, D. Metelko, I. Orehek, P. Čepin, M. Grom, A. Govejšek, M. Pančur, A. Krevl, M.Ciglarič
Različica	1.0
Datum nastanka	17.9.2007
Datum zadnje spremembe	17.9.2007

Kazalo

1. Uvod

Upravljanje identitete uporabnikov in njihovega dostopa do omrežja postaja čedalje pomembnejši izziv za organizacije vseh velikosti. Z izzivom se je soočila tudi Univerza v Ljubljani (UL), ki mora v skladu z Bolonjsko strategijo zagotoviti preprosto prehajanje med posameznimi študijskimi programi, fakultetami in univerzami. Da bi to zagotovili, se je UL odločila za vpeljavo sistema za upravljanje življenjskega cikla identitet.

Upravljanje identitete uporabnikov in njihovega dostopa do omrežja postaja čedalje pomembnejši dejavnik v poslovanju za organizacij vseh velikosti. Organizacije želijo po eni strani učinkovito in varno upravljati z uporabniki ter njihovimi vlogami v organizaciji, po drugi strani se informacije o identiteti redko nahajajo na enotnem mestu. Različni oddelki na različnih lokacijah pogosto uporabljajo različne tehnološke rešitve za upravljanje in shranjevanje identitete, kar otežuje enotno upravljanje z osrednje lokacije. Te slabosti povečujejo stroške organizacije, zmanjšujejo njeno učinkovitost in predstavljajo veliko varnostno tveganje.

2. Obstoječe stanje

Univerza v Ljubljani je sestavljena iz več članic, med katerimi jih večina uporablja različne imenike ali rešitve za upravljanje identitete. Razdrobljenost teh informacij pomeni slabo medsebojno združljivost podatkov o identiteti, obenem pa sistemi med seboj niso povezani, s čimer je izmenjava informacij onemogočena. Poleg tega ni vzpostavljenega enotnega pristopa za izmenjavo informacij o identitetah, kar v praksi pomeni, da je vsaka izmenjava podatkov o identiteti prepuščena posameznim fakultetam, ki so članice Univerze v Ljubljani.

Pomemben izziv je tudi stalna vpeljava novih imenikov za informacije o identiteti, s čimer se še povečuje razdrobljenost in nepovezanost obstoječega sistema. Univerza v Ljubljani prav tako nima vpeljanega enotnega sistema za upravljanje življenjskega cikla identitete. Pri upravljanju le-tega gre za procese ter tehnologije za določanje in odstranjevanje digitalnih identitet ter njihovo upravljanje in sinhronizacijo med

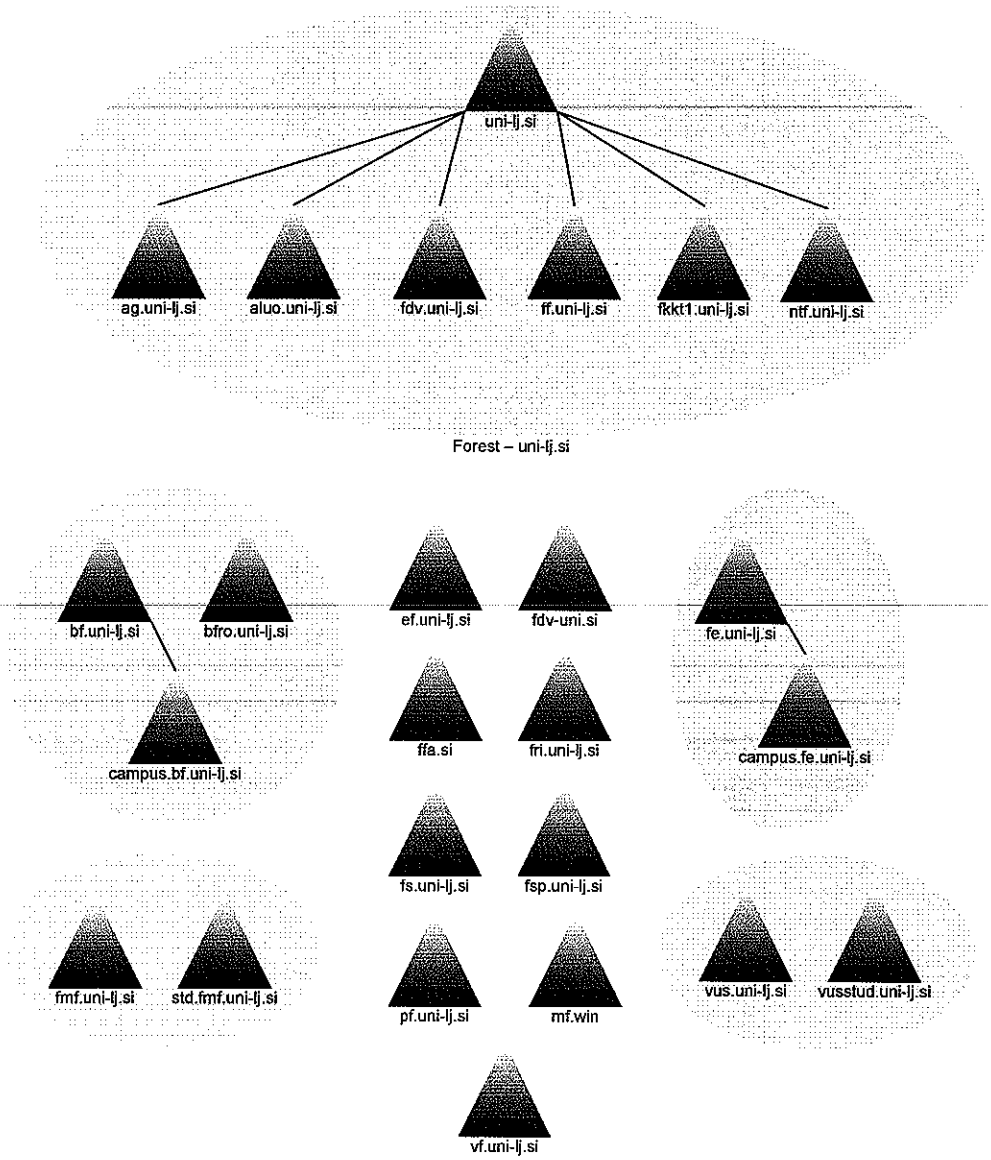
različnimi sistemi. Vse te dejavnosti potekajo od vzpostavitve identitete v sistemu do trenutka, ko je identiteta odstranjena iz sistema.

Vse te slabosti povzročajo velike težave pri dokazovanju identitete ob prehajanju zaposlenih in študentov med fakultetami članicami. Učinkovito dokazovanje identitete je bodisi nemogoče bodisi je povezano z zapletenimi postopki, ki se pogosto ponavljajo in tako povečujejo administrativno obremenitev posameznih fakultet.

2.1. Shema obstoječih imenikov

Trenutno stanje odraža razpršeno delovanje informacijskih služb UL, saj ima 13 članic lastno vzpostavljene imenike, ki niso del gozda UNI-LJ, 6 članic je vključenih v gozd UNI-LJ, preostale članice pa nimajo uvedene imeniške storitve.

Glavna težava obstoječega stanja so poimenovanja domen, saj nekatere članice v imenu svoje domene uporabljajo pripono uni-lj.si, ki je predvidena tudi za vpeljavo novega centralnega imenika.



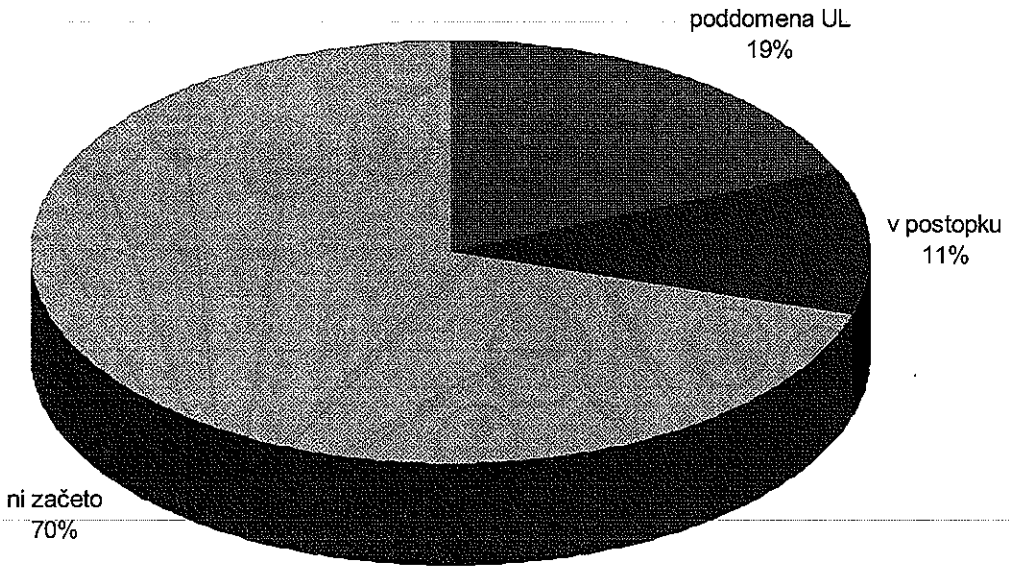
2.2. Imeniške storitve v številkah

Članica	Število zaposlenih	Število študentov	Število računalnikov	Obstoječi AD	Stanje AD
AG	87	436	50	DA	poddomena UL
AGRFT	58	108	50		
ALUO	72	415	50	DA	poddomena UL
BF	605	3768	600	DA	
EF	245	8178	520	DA	
FA	85	994	250		
FDV	249	4614	510	DA	poddomena UL

FE	341	2455	60	DA	
FF	605	7336	600	DA	poddomena UL
FFA	113	1035	220	DA	v postopku
FGG	219	1918	450		
FKKT	208	1762	350	DA	v postopku
FMF	173	1070	300	DA	
FPP	75	1596	90		
FRI	119	1529	40	DA	
FS	319	2178	400	DA	
FSD	56	1223	50		
FŠ	109	1260	220	DA	
FU	74	3609	70	DA	
MF	772	1812	650	DA	
NTF	192	1868	150		v postopku
PEF	194	2656	100		
PF	78	2405	180	DA	
TEOF	70	742	40		
VF	366	435	400	DA	
VŠZ	101	2133	100		
UNI-LJ	100	0	120	DA	domena UL

Ugotavljamo, da je v domeno uni-lj.si že vključenih 19% članic. 11% članic je v postopku pridruževanja domeni uni-lj.si, kar 70% članic pa še ni začelo s pridruževanjem v domeno uni-lj.si, ali pa sploh nimajo implementirane imeniške storitve. Porazdelitev podrobneje prikazuje spodnji graf.

Dodatno težavo pri implementaciji centralne imeniške storitve predstavljajo članice, ki ne želijo pristopiti k uvedbi centralnega sistema za upravljanje identitet. Večinoma navajajo varnostne razloge, vendar pa s tem škodujejo svojim študentom in zaposlencem.



3. Arhitektura predlagane rešitve

Arhitektura upravljanja a identitetami je sestavljena iz treh delov.

- Aktivni imenik
- Sistem za sinhronizacijo podatkov o identitetah z zalednimi sistemi – Identity Lifecycle Manager 2007
- Sistem za upravljanje z digitalnimi potrdili

3.1. Arhitektura aktivnega imenika

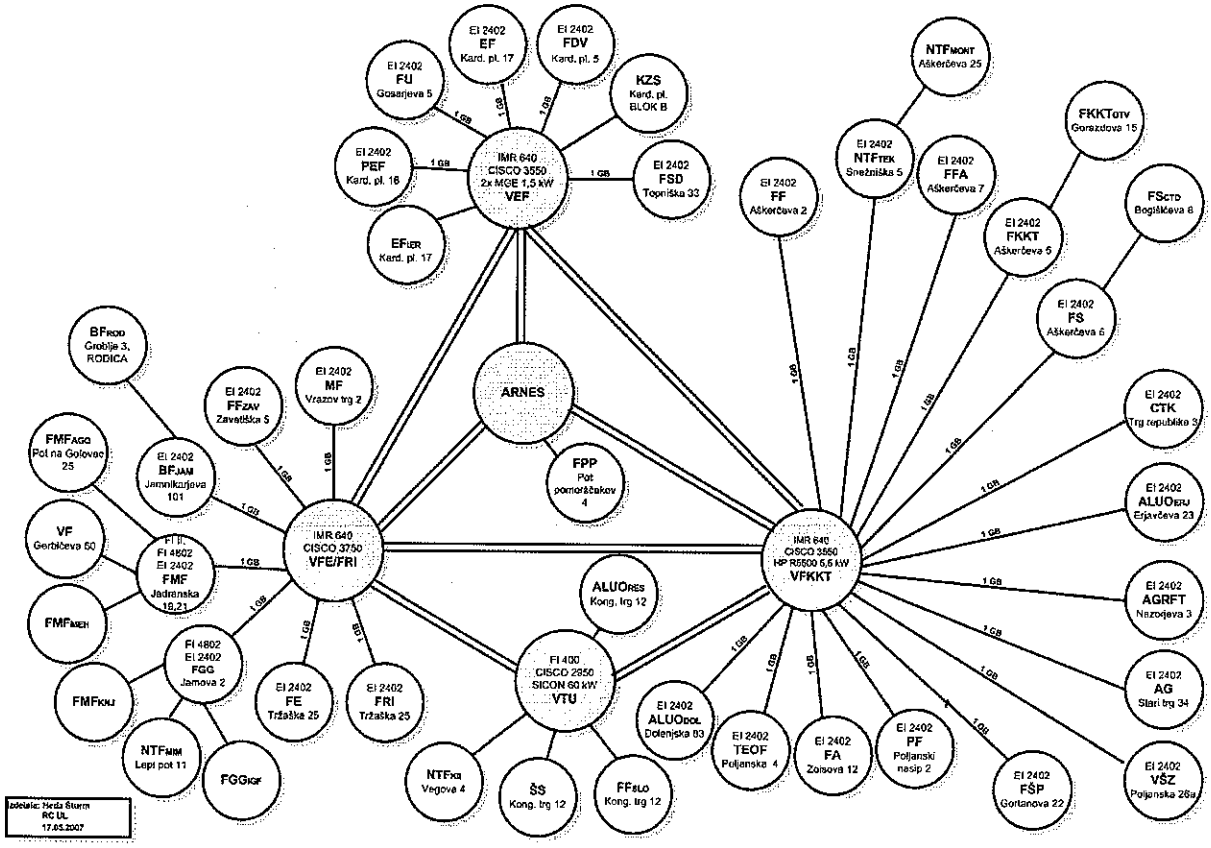
Arhitektura aktivnega imenika je odvisna od naslednjih glavnih elementov:

- Velikostjo samega imenika
- Topologijo omrežja, povezav in oddaljenih lokacij
- Specifičnih zahtev organizacije, ki lahko vpliva na načrtovanje gozda

3.1.1. Velikost imenika

Smiselno je vedeti, približno velikost same baze aktivnega imenika, za planiranje strežnikov in replikacije ter same potrebe po omrežnih povezavah zaradi replikacije domenskih particij. Ocenjena velikost imenika je okoli 15 GB.

3.1.2. Topologija omrežja



Omrežje Univerze v Ljubljani ima več kot dovolj kapacitete za postavitev polne replikacije Aktivnega imenika, saj tudi najpočasnejše povezave med lokacijami dosegajo hitrosti vsaj 768 kbps. Iz tega stališča je najbolj smiselna vzpostavitev enotne domene oz. gozda.

3.1.3. Vloga OP

Domenski strežniki v Active Directoy so enakovredni in si replicirajo vse spremembe med seboj. Replikacija nekaterih specifičnih informacij (na primer spreminjanje sheme, dodajanje novih domen, itd...) na tak način ni praktična. Za repliciranje takšnih informacij so zadolženi domenski strežniki, ki ob običajnih nalogah opravljajo tudi posebne vloge, imenovane Operations master. Takšnih vlog je pet (5). Dve na nivoju gozda ter tri v vsaki domeni. Na nivoju gozda sta dve vlogi:

- Schema master
- Domain naming master

Na nivoju domen so tri vloge:

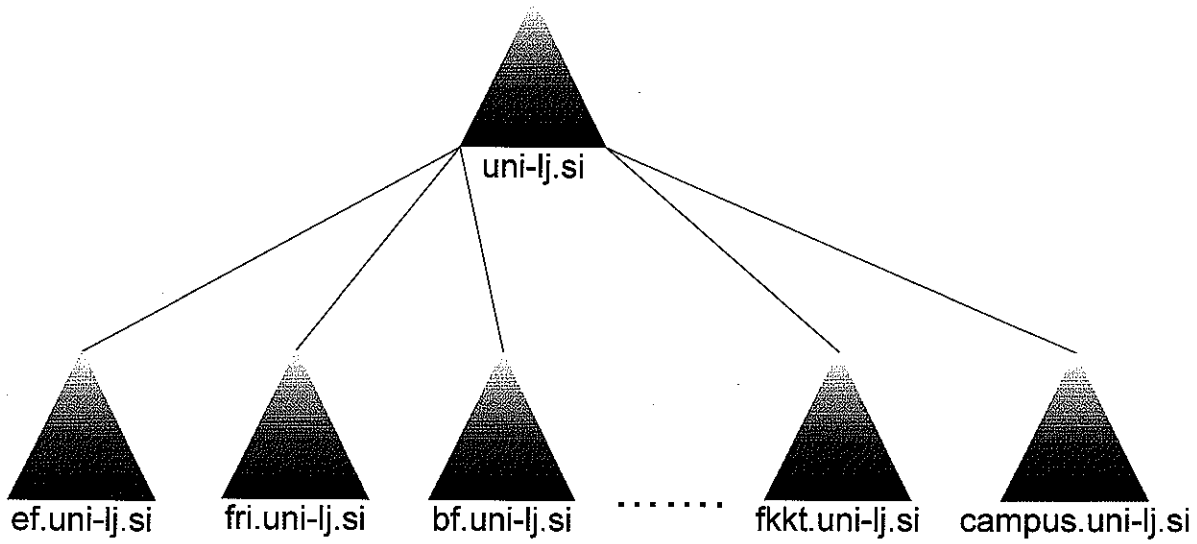
- Relative ID (RID) master.
- Primary Domain Controller (PDC) master
- Infrastructure master

3.1.4. Vloga GC

Globalni katalog je posebna vloga v Active Directory. Domenski strežniki s to vlogo hranijo delne kopije vseh objektov Active Directory gozda, ki so na voljo za iskanje odjemalcem. GC je privzeto omogočen na prvem domenskem strežniku v domeni in skrbi za naslednja opravila:

- Iskanje. GC se uporabi pri iskanju domenskih objektov (uporabnikov, računalnikov, skupin, itd..) znotraj gozda.
- User Principal Name (UPN) razreševanje. GC razrešuje UPN imena (ime@domena) pri prijavi, kadar lokalni domenski strežnik imena ne prepozna - na primer kadar se uporabnik iz domene1 prijavi na računalniku, ki je v domeni2 in za prijavo uporabi ime@domena1.
- Članstvo v univerzalnih skupinah v večdomenskem okolju. Ob prijavi uporabnika se zgradi njegov žeton s članstvi v vseh skupinah. Podatki o članstvu v Univerzalnih skupinah so shranjeni samo v GC. Če ob prijavi GC ni na voljo in se je uporabnik prej že prijavil v domeno na tem računalniku se uporabijo "cached credentials". Če se uporabnik na tem računalniku ni prijavil v domeno in GC ni na voljo, se uporabnik ne more prijaviti z domenskim računom. Izjema je račun Administrator, ki se vedno lahko prijavi v domeno - tudi če GC ni dosegljiv.
- Preverja veljavnost referenc med objekti v gozdu. Kadar objekt vsebuje referenco na objekt, ki se nahaja v drugi domeni se veljavnost reference preverja v globalnem katalogu.
- Ostale storitve aplikacij, kot je na primer iskanje po Exchange imeniku.

3.1.5. Arhitektura imenika



V novem sistemu za upravljanje digitalnih identitet bodo vse članice del enega gozda. Ime gozda univerze bo uni-lj.si, ostale poddomene članic pa bodo sledile dosedanjemu imenovanju (npr. fri – Fakulteta za Računalništvo in Informatiko).
Celoten gozd bo deloval v Windows Server 2003 načinu, kar pomeni, da bodo tudi vse ostale domene delovale v tem načinu. V gozdu ne bo nobenega strežnika, ki bi imel nameščen operacijski sistem Windows 2000 ali starejši.

3.1.6. Študentska domena

V okviru celotne arhitekture, bo postavljena ločena domena, ki bo namenjena računom za študente. Ti računi bodo v uporabi za potrebe dostopov študentov do različnih virov (eStudent G3), laboratorijev ipd.

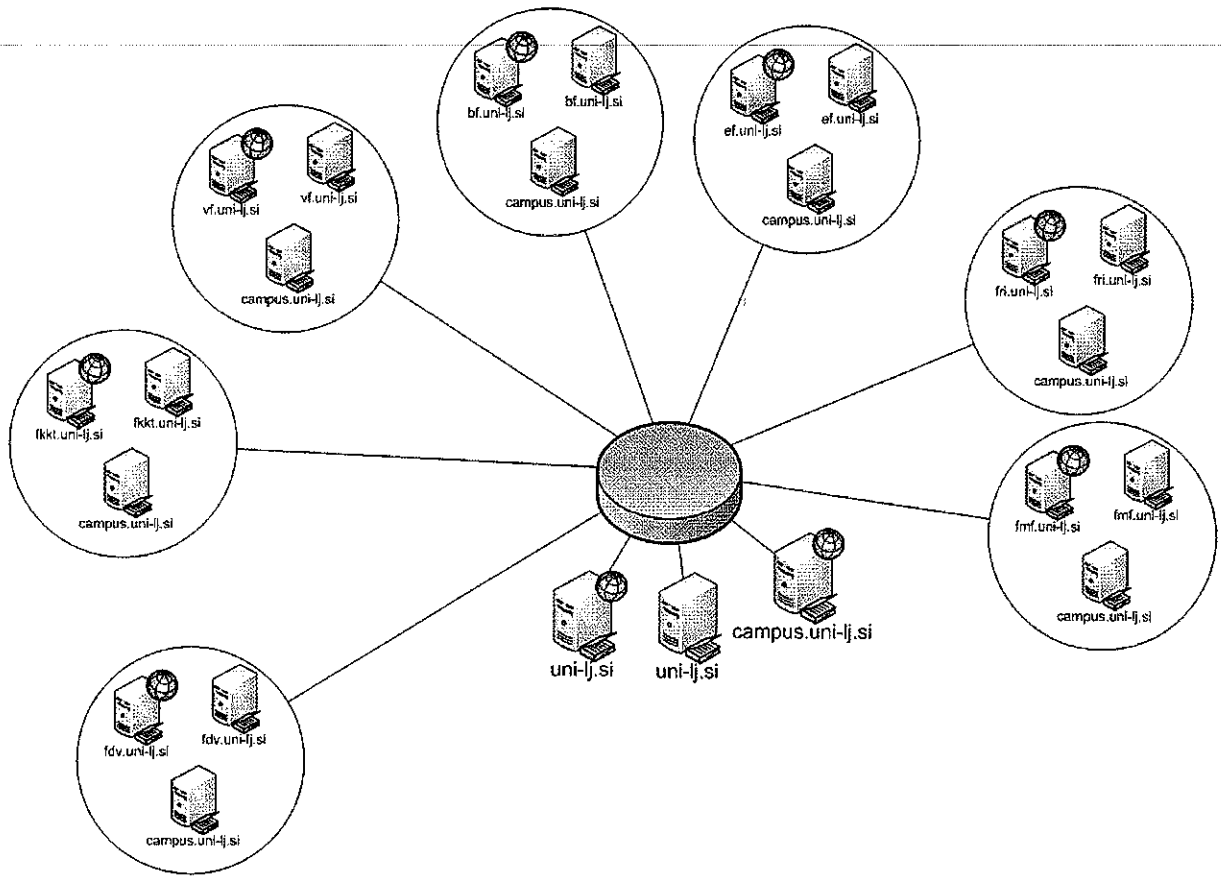
Domena student.uni-lj.si bo umeščena kot del gozda uni-lj.si in bo gostila vse račune študentov (okoli 50.000). Zato da bo avtentikacija potekala nemoteno, bo na vsaki članici nameščen domenski strežnik za domeno student.uni-lj.si.

Študentska domena je organizirana po organizacijskih enotah glede na posamezno članico. S tem se posamezni članici lahko delegirajo pravice upravljanja določenega študenta, ki je vpisan v določeni članici. Študentski računi se nahajajo v posameznih organizacijskih enotah znotraj domene student.uni-lj.si.

3.1.7. FSMO vloge

Glede na predlagano arhitekturo, naj bodo FSMO vloge porazdeljene na naslednji način:

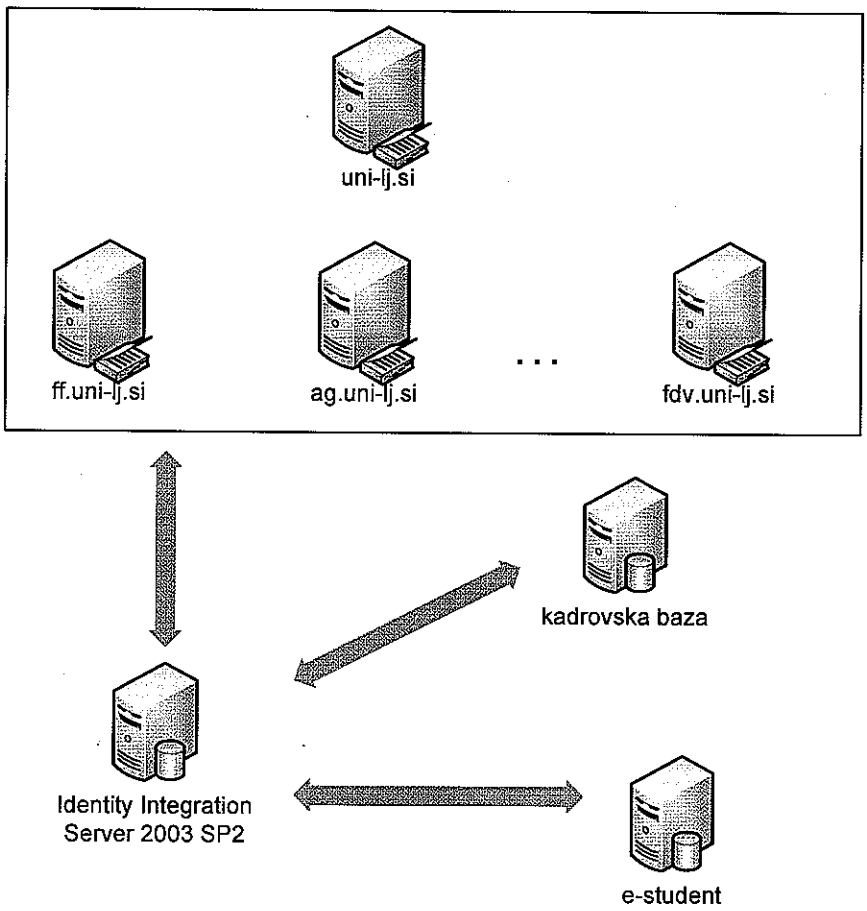
- Vrhnja domena uni-lj.si ima vlogi Shema master in Domain Naming Master
- Vsaka domena bo na svoji lokaciji na istem strežniku gostila PDC, RID in Infrastructure master
- Strežnik, ki bo imel vse vloge ne bo globalni katalog (GC)



3.2. Sistem za sinhronizacijo podatkov o digitalnih identitetah

Namen sistema sinhronizacije digitalnih identitet je, da se različni podatki o identitetah pretakajo iz zalednih sistemov v imenik in nazaj. Sistem je samo vmesni člen, ki omogoča tok podatkov. V projektu je predvidena vzpostavitev toka podatkov iz sistemov eStudent ter kadrovskih baz v aktivni imenik.

Kot je prikazano v sliki spodaj se sistem povezuje z aktivnim imenikom, katerega oskrbuje z podatki o zaposlenih in študentih. Kateri podatki se prenašajo je odvisno od različnih pravil varovanja zasebnosti ter atributov, ki se hranijo v zalednih sistemih. Določitev toka sinhronizacije je cilj naslednjih faz projekta.



Za samo delovanje sinhronizacije bomo uporabili Identity Lifecycle Manager 2007, ki omogoča povezovanje z različnimi viri podatkov ter le te glede na pravila usklajevati med različnimi izvori/ponori podatkov.

Ključno je, da se pred vzpostavitvijo sistema sinhronizacije najprej vzpostavi osnovna infrastruktura DNS/DHCP strežnikov ter Aktivnega imenika.

3.3. Sistem za upravljanje digitalnih potrdil

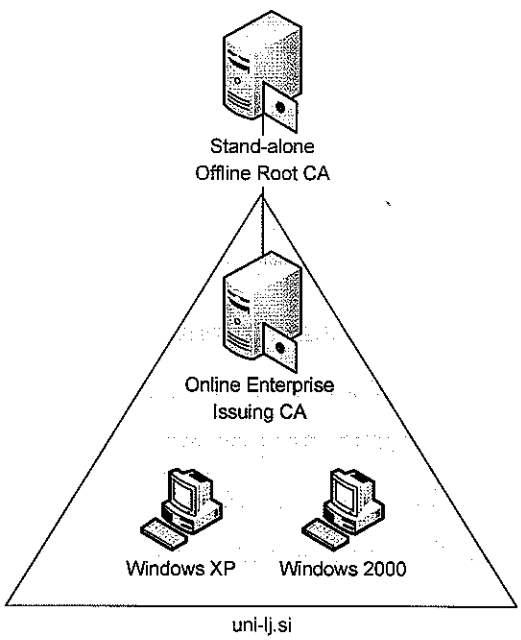
Kot del projekta upravljanja z digitalnimi identitetami, se bo vzpostavila osnovna arhitektura strežnikov za izdajo digitalnih potrdil. Digitalna potrdila so eden od ključnih storitev, ki jih lahko Univerza ponudi študentom in zaposlenim, saj omogočajo napredne varnostne scenarije v omrežju univerze kot so:

- Varna prijava na računalnike v omrežju
- Izdaja pametnih kartic, ki identificirajo študente pri interakciji z različnimi sistemi
- Izdaja digitalnih potrdil za strežnike znotraj omrežja

3.3.1. Strežniki za izdajo digitalnih potrdil

Arhitektura rešitve predvideva postavitev dvo nivojske CA (Certification Authority) topologije v testnem okolju:

- *Stand-alone offline root CA:* zaradi varnosti ta strežnik ni nikoli povezan z mrežo in ni član domene. Razumljivo je, da mora ostati ta strežnik fizično zavarovan. Root CA izdaja in zavrača certifikate za »Online Enterprise Issuing CA«. Certifikati in CRL (Certificate Revocation List) so ročno objavljeni na HTTP ali LDAP distribucijski točki.
- *Online Enterprise Issuing CA:* Ta strežnik je član domene in je odgovoren za izdajo certifikatov končnim uporabnikom. Strežnik je vedno priključen na mrežo in je član domene. Fizična varnost strežnika, je tudi v tem primeru pomembna.



4. Načrt za uvedbo

Osnovno vodilo načrta je, da je v vsaki domeni zadostno število strežnikov DC za zagotavljanje naslednjih zahtev:

- zagotavljanje ustreznih odzivnosti za odjemalce (razpoložljivost);
- zagotavljanje odpornosti na napake (redundanca);

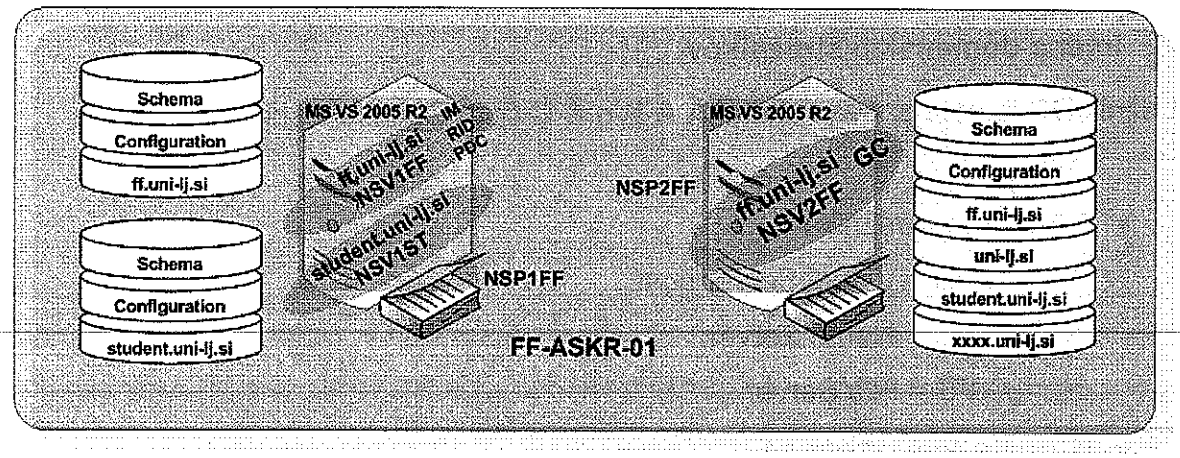
Odzivnost za odjemalce je pogojena tako s procesorsko močjo samih strežnikov kot tudi z omrežno prepustnostjo med odjemalci in strežniki DC.

Načrt ne predvideva uporabe prijavnih skript, pri katerih prihaja do prenosov večjih datotek med strežnikom in odjemalcem.

Načrt predvideva:

- V korensko domeno »**uni-lj.si**« so postavljeni 3 strežniki DC. 2 strežnika nosita vlogo DNS in sta umeščena v različna območja.
- V vsako domeno članice se postavi vsaj 2 fizična strežnika za podporo vlogi DC.
- Na vsako območje se postavi en strežnik DC z vlogo GC.
- Vsaj en strežnik DC se postavi v virtualizirano okolje Microsoft Virtual Server.
- Vloge FSMO na nivoju gozda so postavljene na strežnik DC na območju uprave.
- Vloge FSMO na nivoju domene so postavljene na strežnik DC, ki ne nosi vloge GC.
- Na oddaljena območja članic zunaj omrežja METULJ, ki ne zagotavljajo vsaj 50KB pasovne širine na uporabnika do omrežja METULJ, se postavi lastno območje. Na takšno lokacijo se postavi »mini« domenski strežnik, ki ne opravlja vloge GC. Zagotovi se predpomnjenje članstva v univerzalnih skupinah (»**Universal Group Membership Caching**«).
- Na območje uprave se postavi 1 strežnik (bodisi fizičen ali virtualiziran) z vlogo DC za podporo študentski domeni.

- V vsako primarno območje članice se postavi 1 virtualiziran strežnik z vlogo DC za podporo študentski domeni.
- Skupno se za domene 26 članic in študentsko domeno predvideva 52 fizičnih strežnikov, ki podpirajo funkcije domene.



4.1. Programska oprema

Uvedba centralnega sistema za upravljanje identitet predvideva naslednjo programsko opremo:

- Microsoft Windows Server 2003 R2, x64, Enterprise Edition
- Microsoft Virtual Server 2005 R2
- Microsoft Windows Server 2003 R2, Standard Edition

4.2. Strojna oprema

Uvedba centralnega sistema za upravljanje identitet predvideva naslednjo strojno opremo za gostiteljski strežnike:

- CPU: 1 x Dual-Core
- RAM: 4 GB
- HDD: 2 x 146 GB SAS
- NIC: 4 x 1Gb

Za strežnike DC, ki bodo to vlogo opravljali na dislociranih lokacijah članic, priporočamo enak model strežnika z nižjimi kapacitetami.

- CPU: 1 x Dual-Core
- RAM: 1 GB
- HDD: 2 x 146 GB SAS
- NIC: 1 x 1Gb

4.3. Imena domenskih strežnikov

Strežnik DC je poimenovan shemi **A A B n C C C C**. Oznake v shemi pomenijo:

- AA - Vloga strežnika
  - VS = Virtual Server host
  - NS = Name Server
  - FS = File Server
- B – umestitev strežnika
  - P = OS na fizičnem strežniku
  - V = OS kot gost v virtualiziranem okolju
- n – zaporedna številka
- CCCC – oznaka članice

5. Zaključek

Načrt vpeljave centralnega sistema za upravljanje z digitalnimi identitetami (AD) na Univerzi v Ljubljani zagotavlja, da se informacije o objektih v imeniku regularno replicirajo prek celotnega informacijskega okolja. Informacije, objavljene v imeniku so zato konsistentne in vedno na voljo postajam oziroma uporabnikom.

Načrt je prilagojen omrežni topologiji in infrastrukturi Univerze v Ljubljani in zagotavlja, da imajo postaje in strežniki v omrežju na voljo dovolj dober odziv strežnikov za avtentikacijo ter zagotovljeno možnost avtentikacije in prijave tudi v primeru okvare strežnika DC.

UVAJANJE ENOTNEGA UPRAVLJANJA Z DIGITALNIMI IDENTITETAMI NA UNIVERZI V LJUBLJANI

Andrej Krevl, Matjaž Pančur, Mojca Ciglarič

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Tržaška 25, Ljubljana

Andrej.Krevl | Matjaž.Pancur | Mojca.Ciglaric@fri.uni-lj.si

Povzetek

Današnje informacijske sisteme sestavlja nabor različnih aplikacij, ki večinoma uporabljajo lastne avtorizacijske in avtentikacijske mehanizme. Zaradi tega so uporabniki soočeni z množico uporabniških imen in gesel, ki jih uporabljajo za dostop do različnih storitev informacijskega sistema. Neželeni posledici navedenega sta nepotrebno obremenjevanje uporabnikov in varnostno tveganje, saj si uporabniki množico gesel težko zapomnijo. Članek opisuje izkušnje, ki jih je Univerza v Ljubljani pridobila z odločitvijo, da vzpostavi enoten sistem za upravljanje z digitalnimi identitetami zaposlenih in študentov. Pojasnjeni so osnovni pojmi, opisano je staro stanje na področju digitalnih identitet, predstavljen je potek vzpostavitve in prehoda na sistem za upravljanje z digitalnimi identitetami, pojasnjene so tudi izbrane načrtovalske odločitve.

Abstract

INTRODUCING DIGITAL IDENTITY MANAGEMENT AT UNIVERSITY OF LJUBLJANA

Modern information systems consist of many applications, each of them using own authorization and authentication mechanisms. Users have to deal with a set of usernames and paswords when trying to access different information services. Since users sometimes write down their passwords and keep them in insecure places, this represents a security risk to the system The paper decribes experiences gained by building unified digital identity management system at University of Ljubljana.We explain the relevant definitions, describe the situation, summarize the project plan and discuss a few design choices.

Ključne besede

Digitalna identiteta, sistem za upravljanje z digitalnimi identitetami, imenik, sinhronizacija

Key words

Digital identity, digital identity managment system, directory, synchronisation

1. UVOD

Informacijski sistemi Univerze v Ljubljani so razpršeni po članicah (fakultetah, oddelkih, pisarnah...), ki imajo poleg maloštevilnih skupnih aplikacij specifičen nabor lastnih aplikacij, ki z aplikacijami drugih članic niso združljive in uporabljajo svoje avtentikacijske in avtorizacijske sisteme.

S postopnim uvajanjem bolonjskega študija se povečuje mobilnost študentov in profesorjev, ki potrebujejo dostop do univerzitetne informacijsko komunikacijske infrastrukture tudi na drugih lokacijah, ne le na svoji matični, zato se število njihovih digitalnih identitet še

povečuje kljub dejstvu, da tehnologija omogoča, da bi vsak posameznik tudi v velikem in kompleksnem sistemu imel le eno digitalno identiteto.

Dolgoročni cilj Univerze v Ljubljani je vzpostavitev centralnega sistema za upravljanje digitalnih identitet za celotno Univerzo v Ljubljani – za vse zaposlene in tudi vse študente. Ta sistem bo podatke o identitetah zajemal iz obstoječih podatkovnih baz, in sicer glavnino iz postopka vpisa na univerzo in iz kadrovske evidence. Upravljal bo z identitetami za obstoječe storitve informacijskega sistema Univerze, hkrati pa bo omogočil razvoj novih storitev, kot so enotna elektronska pošta za študente, dopisni seznami, skupni koledarji in centralni imenik. Poenostavil bo administracijo digitalnih identitet in razbremenil skrbnike informacijskih sistemov na fakultetah, obenem pa ustrezno poskrbel za varnost.

2. IZHODIŠČA IN OPIS PROBLEMATIKE

Navedimo najprej definicije pojmov, ki so pomembni v kontekstu upravljanja z identitetami.

Po [1] je **identiteta** osebka tista množica atributov, ki ga identificira znotraj neke množice osebkov. Ker so množice osebkov lahko zelo različne, tudi ta množica atributov ni enaka v vsaki množici osebkov. Lahko torej trdimo, da osebek nima ene unikatne identitete, ampka celo množico identitet. Vrednosti atributov in tudi sami atributi se lahko s časom spreminjajo, torej se nujno spreminjajo tudi identitete.

Vloga (role) je množica akcij ali tudi pričakovano obnašanje osebka v določenih okoliščinah. Delna identiteta osebka, ki ji lahko ustreza psevdonim osebka (oziroma eden od psevdonimov), pa je tista podmnožica atributov celotne identitete, ki predstavlja ta osebek v določeni vlogi.

Digitalna identiteta osebka je množica tistih atributov osebka, ki so shranjeni, povezani in dosegljivi s pomočjo računalniške tehnologije.

Upravljanje z identitetami s pomočjo tehnologije se v najširšem smislu nanaša na načrtovanje in upravljanje podatkov, ki sestavljajo digitalno identiteto. **Sistem za upravljanje z digitalnimi identitetami** je infrastruktura, kjer se usklajeno uporabljajo različne aplikacije in orodja (odjemalska ali strežniška) za upravljanje z identitetami. Takšen sistem omogoča razpoznavanje različnih vrst komunikacije in različnih situacij ter jih vrednoti glede na pomen, funkcionalnost, tveganje glede na varnost in zasebnost. Glede na tu opredeljuje, dodeljuje in uporablja ustrezne vloge.

S svojo digitalno identiteto se uporabnik prvič sreča ob prijavi na računalnik. Čeprav preverjanje uporabniškega imena in gesla samo po sebi ni težko opravilo, pa so pravi sistemi za upravljanje digitalnih identitet kompleksni in jih uspešno uporabljajo le redke organizacije.

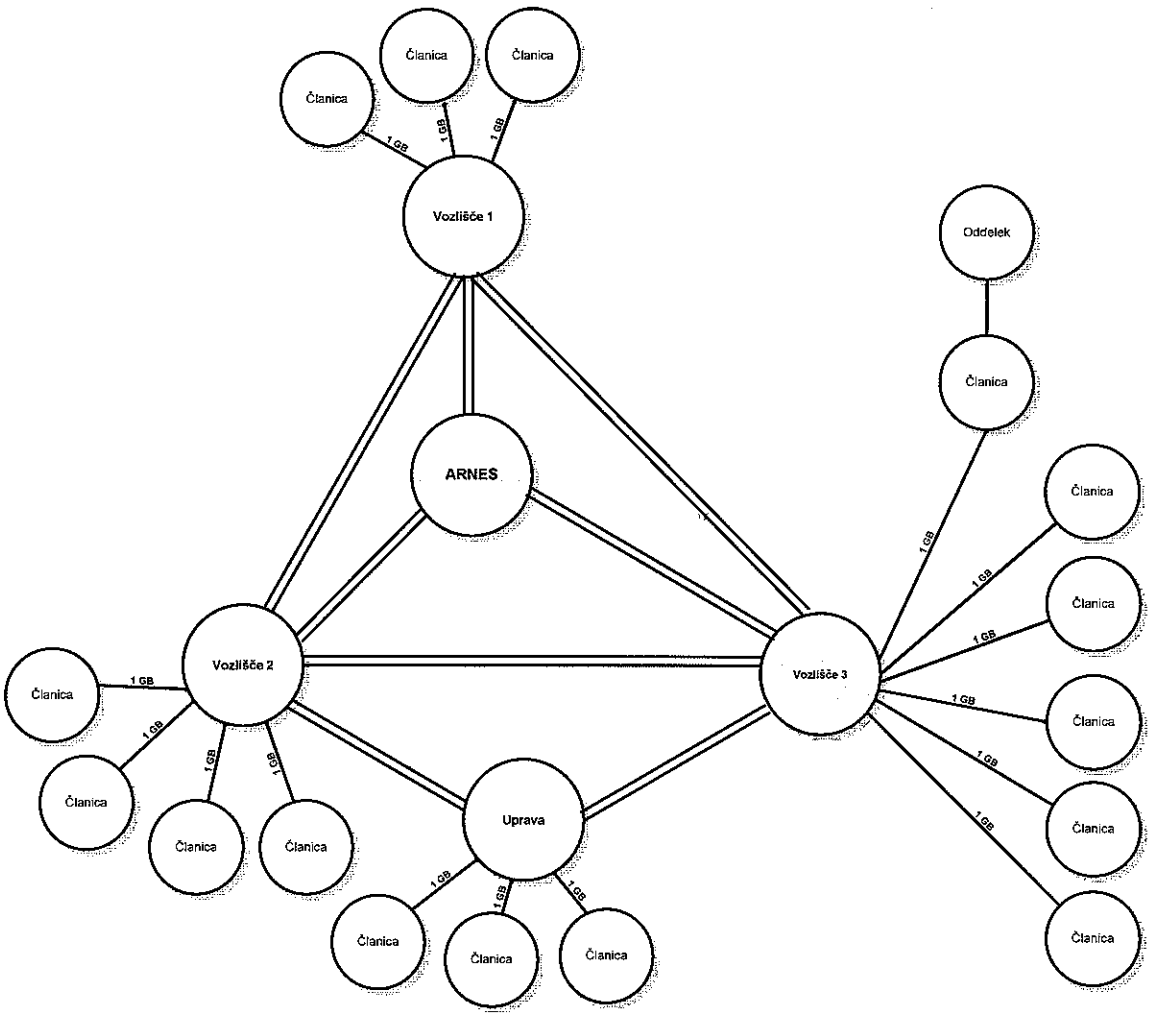
Informacijski sistem Univerze v Ljubljani ima več kot 70.000 uporabnikov (zaposlenih in študentov), razpršenih po članicah in na upravi Univerze. Ti uporabniki vsakodnevno dostopajo do informacijskega sistema in zahtevajo dostop do različnih storitev v okviru svoje fakultete, univerze, kot tudi do storitev, ki jih nudijo partnerske inštitucije.

Članice v svojem okolju uporabljajo različne tehnologije, zato imajo uporabniki za dostop do različnih storitev praviloma ločena uporabniška imena in tako različne delne identitete. Za dostop do računalnikov v računalniških učilnicah se za študente marsikje uporabljajo skupinska uporabniška imena, ki si jih delijo cele generacije ali celo več generacij. Sinhronizacije uporabniških imen in gesel med različnimi sistemi praktično ni, zato o sistemih

za upravljanje digitalnih identitet v pravem pomenu še ne moremo govoriti. Za storitve, pri katerih je zahtevana višja stopnja varovanja podatkov, se navadno uporabljajo sistemi kriptografije z javnimi ključi, ki se opirajo na zunanje certifikatne agencije (npr. SIGEN). Večina članic (fakultet) ima na svoj način rešeno upravljanje uporabniških imen za lastne zaposlene, za študente pa na veliko članicah ne obstaja niti skupni imenik.

Z vpeljavo bolonjskih študijskih programov se povečuje mobilnost študentov, ki dostopa do storitev ne zahtevajo le v okviru fakultete na katero so se vpisali, ampak tudi v okviru drugih fakultet. Nove storitve, kot je na primer brezžično omrežje Eduroam, že v osnovi omogočajo prehajanje študentov med različnimi organizacijami - tudi v tujini. Tudi te storitve zahtevajo imenike, avtentikacijske in avtorizacijske mehanizme, ki jih je potrebno redno dopolnjevati in spreminjati.

Opisana izhodišča jasno kažejo, da je na Univerzi potrebno zasnovati sistem za upravljanje z digitalnimi identitetami. Ta sistem mora omogočati sinhronizacijo delnih digitalnih identitet iz različnih obstoječih imenikov med seboj, podpirati mora prehajanje osebja med članicami in drugimi partnerskimi ustanovami, opreti pa se mora na podatkovne zbirke, ki že vsebujejo podatke o zaposlenih in o študentih na univerzi.



Slika 1: Hrbtenica univerzitetnega omrežja Metulj

Pred nedavnim nadgrajeno univerzitetno omrežje predstavlja prvi korak, ki omogoča vzpostavitev skupnega sistema za upravljanje identitet v okviru celotne univerze. Vendar pa

je zaradi občutljivosti podatkov, ki se nahajajo v teh sistemih, potrebno skrbno načrtovanje prehoda na skupni sistem, ki mora biti v skladu z veljavnimi predpisi in varnostnimi standardi (zlasti ISO 27001:2005), upoštevati pa mora tudi najboljše prakse pri upravljanju informacijskih procesov (npr. ITIL), saj bo le tak sistem vzpostavil primerno mero zaupanja s strani članic in s strani uporabnikov sistema.

Enoten sistem za upravljanje digitalnih identitet bo omogočil razvoj novih storitev kot so skupni koledarji, centralni imenik elektronskih naslovov, omogočanje dostopa do infrastrukture na članicah, dostop do knjižničnih gradiv in podobno. Rezultati projekta pa so pomembni tudi za uspešen zaključek drugih razvojnih projektov Univerze.

Opisani sistem bo omogočil tudi vzpostavitev certifikatne agencije na nivoju univerze, saj pri uporabi certifikatov drugih agencij lahko nastopijo organizacijske težave (npr. ko je posamezni certifikat potrebno preklicati). V skladu s politiko Univerze pa bo seveda potrebno omogočiti tudi navzkrižno overjanje ali povezljivost s tujimi univerzitetnimi in raziskovalnimi inštitucijami, kar bo povečalo konkurenčnost in olajšalo mobilnost (v obe smeri – slovenskih in tujih) študentov in profesorjev.

3. POTEK PROJEKTA

Vzpostavitev sistema za upravljanje digitalnih identitet na nivoju Univerze je velik organizacijskih in tehnični izziv tudi zaradi heterogenosti infrastrukture, s katero je potrebno zagotoviti povezljivost, zaradi velike množice uporabnikov ter značilnosti njihove organiziranosti. Menimo, da bodo tudi zaradi tega izkušnje, pridobljene na projektu, zanimive za širšo javnost v Sloveniji, pa tudi v tujini.

Sama izvedba projekta je načrtovana v več fazah, ki jih vsebinsko lahko delimo v devet točk:

1. Izdelava analize, primerjava in izbira najprimernejšega sistema za upravljanje digitalnih identitet
2. Izdelava načrta za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
3. Priprava strategije prehoda na integriran sistem za upravljanje digitalnih identitet, celovito zaščito in varovanje identitete
4. Priprava ITIL procesov za upravljanje z digitalnimi identitetami
5. Vzpostavitev centralnega imenika na upravi Univerze in povezovanje z obstoječimi sistemi (Vpis, Kadrovska evidenca...)
6. Pilotna vključitev ene manjše akademije in ene večje fakultete v sistem za upravljanje z digitalnimi identitetami
7. Testiranje delovanja in odpravljanje morebitnih napak
8. Postopna vključitev preostalih članic v sistem za upravljanje z digitalnimi identitetami.
9. Vzpostavitev univerzitetne certifikatne agencije

Za izvedbo imenika je bila izbrana Microsoftova platforma, središče sistema bo tako osrednji aktivni imenik (Active Directory), prek katerega se bodo pri dostopu do standardnih informacijskih storitev Univerze avtenticirali tako študentje kot tudi zaposleni.

Projektna skupina je najprej analizirala obstoječe stanje na UL, saj posamezne članice (fakultete,...) vodijo podatke o identitetah uporabnikov na heterogene načine, v različnih imeniških sistemih, ki so med seboj težko združljivi. Pri prehajanju med inštitucijami je zato v

zatečenem stanju zaposlenim in študentom dokazovanje identitete otežkočeno ali pa povezano z zapletenimi administrativnimi postopki. Ugotovljeno je bilo, da ima približno polovica članic lastne imenike, četrtina je vključenih v obstoječo univerzitetno domeno, preostale pa imeniške storitve nimajo implementirane.

Arhitektura bodoče rešitve sestoji iz treh ključnih delov: osrednjega aktivnega imenika, sistema za sinhronizacijo podatkov o identitetah z zalednimi sistemi in sistema za upravljanje z digitalnimi potrdili. Ključna aktivnost v začetnih fazah projekta pa je bil razvoj načrta za uvedbo sistema. V njem so postavljene zahteve po ustrezni odzivnosti (razpoložljivost) in odpornosti na napake, ovrednotene so infrastrukturne zahteve – računalniki ter ustrezna programska in strojna oprema, standardi poimenovanja in podobno. Načrt zagotavlja, da se bodo imeniški podatki pravilno replicirali po sistemu in bodo zato vedno na voljo uporabnikom. Prilagojen je omrežni topologiji in obstoječi komunikacijski infrastrukturi UL, zato zagotavlja tudi ustrezno odzivnost in robustnost.

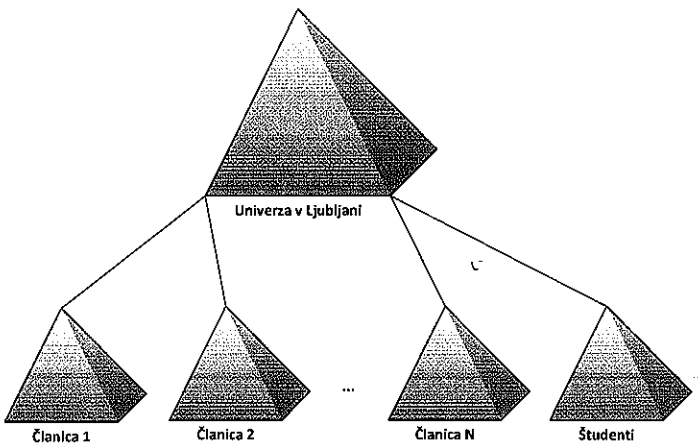
Naslednja ključna aktivnost je bila priprava strategije prehoda na integriran sistem za upravljanje digitalnih identitet, ki vključuje tudi celovito zaščito in varovanje identitete. Strategija zajema naslednja področja:

a) Poimenovanje objektov v centralnem imeniku
b) Migracija digitalnih identitet zaposlenih iz obstoječih imenikov v nov centralni imenik
c) Ustvarjanje in upravljanje digitalnih identitet za študente UL
d) Ustvarjanje in upravljanje digitalnih identitet za zaposlene na UL
e) Preslikava in usklajevanje atributov med imenikom in zalednimi sistemi
f) Priporočila za razvoj novih aplikacij

V času pisanja tega prispevka je osrednji imenik že postavljen, projekt pa je v zelo občutljivi fazi, ko članice postopno migrirajo obstoječe uporabniške račune iz starih domen.

4. OPIS SISTEMA ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI

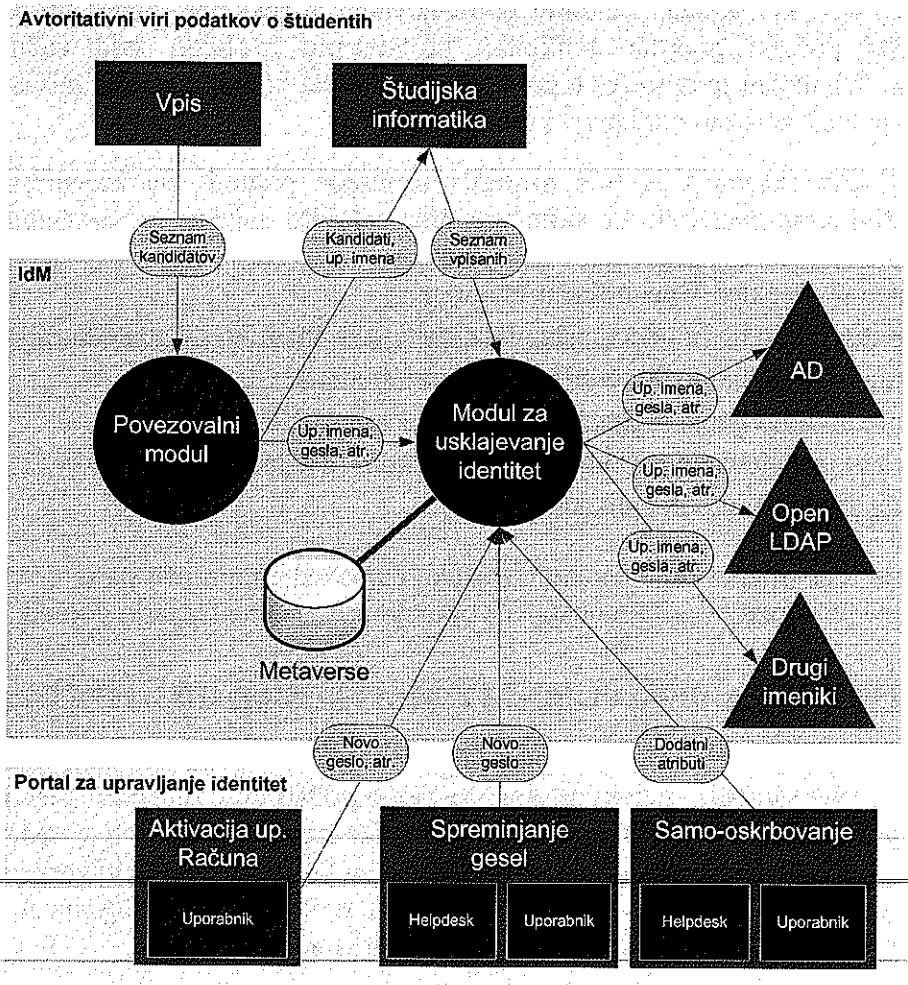
Končni cilj, torej celoten sistem za upravljanje z digitalnimi identitetami, ima tri ključne komponente: aktivni imenik, sistem za sinhronizacijo podatkov z zalednimi sistemi in sistem za upravljanje z digitalnimi potrdili. Na arhitekturo aktivnega imenika vpliva več faktorjev, na primer sama velikost imenika (podatkovne baze) – ta je na primeru Univerze ocenjena na velikost okrog 15 GB podatkov, pomembna je tudi topologija in zmogljivost omrežja, ne nazadnje pa so tu še specifične zahteve in potrebe akademskega okolja.



Slika 2: Univerzitetni gozd

Ker je omrežje redno posodabljano in nadgrajevano, je tudi njegova kapaciteta visoka in omogoča popolno replikacijo podatkov.

Vsaka članica ima svoj domenski strežnik in ti strežniki si med seboj replicirajo imeniške podatke. Skrbno izbrani domenski strežniki poleg teh izvajajo še specifične dodatne funkcije, kot so na primer glavni domenski nadzornik, globalni katalog in podobno. Domene vseh članic so del istega gozda, imenski strežniki članic so z vidika operacijskega sistema homogeni. Ločeno je vzpostavljena še študetska domena, namenjena za delo po učilnicah, za dostop do študijske informatike, za dostop do brezžičnega omrežja Eduroam in drugih storitev, namenjenih študentu. Domenski strežniki te domene so replicirani po vseh članicah.

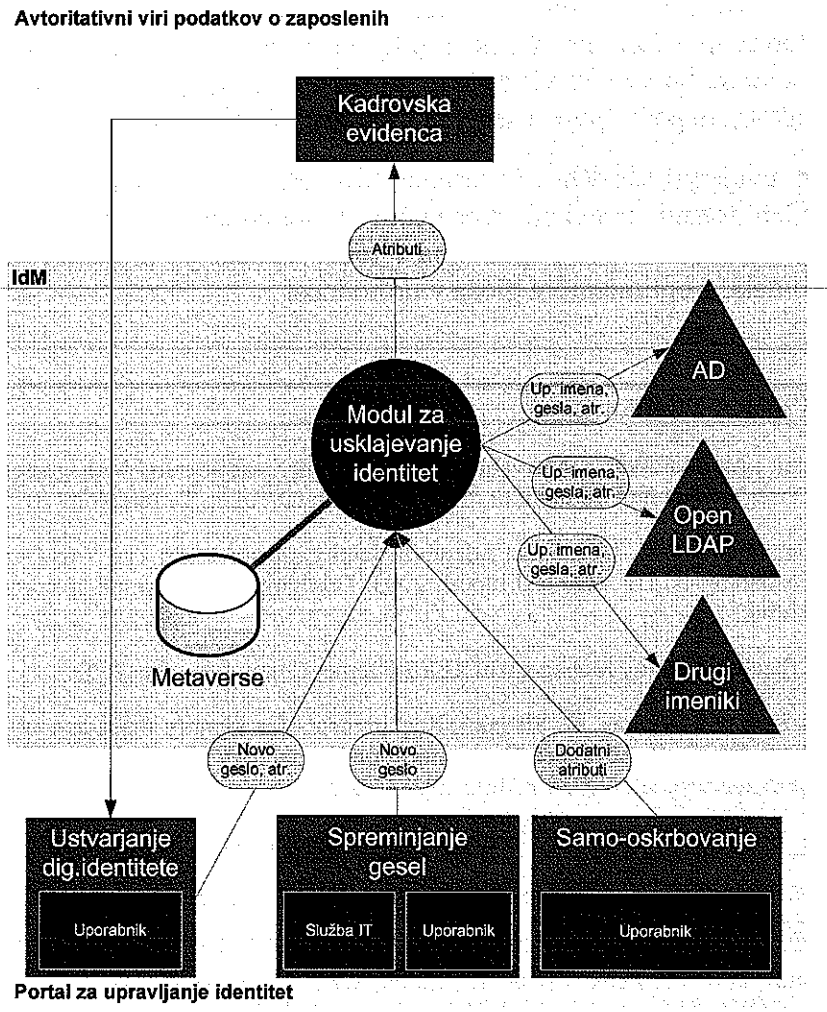


Slika 3: Usklajevanje podatkov o študentih

Proces polnjenja aktivnega imenika s podatki hranita dva tokova podatkov – iz procesa vpisa in iz kadrovske informatike. Vsebina prenosa, torej konkretni atributi polnjenja aktivnega imenika in tudi sinhronizacije med strežniki, je omejena z na različnih nivojim postavljenimi pravili varovanja zasebnosti in omejevanja dostopa do podatkov.

Pred zagonom sinhronizacije sistemov mora biti postavljen aktivni imenik ter ustrezni domenski strežnik(i). Določena morajo biti tudi vsebinska pravila igre – kaj, kako, kdaj usklajevati. Namen sinhronizacije je nadzorovano pretakanje in usklajevanje podatkov o digitalnih identitetah med različnimi zalednimi sistemi in osrednjim aktivnim imenikom.

Tretja komponenta sistema za upravljanje z digitalnimi identitetami je osnovna arhitektura strežnikov za izdajo digitalnih potrdil. Digitalna potrdila so ena od ključnih storitev, ki jih lahko Univerza ponudi študentom in zaposlenim, saj omogočajo napredne varnostne scenarije v omrežju Univerze. Primeri takšnih scenarijev so v današnjem nevarnem internetu že samoumevni - denimo varna prijava na računalnike v omrežju, uporaba pametnih kartic, ki identificirajo uporabnike pri interakciji z različnimi sistemi, izdaja digitalnih potrdil za strežnike znotraj omrežja in podobno.



Slika 4: Usklajevanje podatkov o zaposlenih

Arhitektura rešitve predvideva vzpostvitev dvonivojske certifikatne avtoritete: prvi nivo predstavlja samostojni korenski strežnik, ki ni povezan v omrežje in izdaja digitalna potrdila v omrežje povezanim strežnikom - izdajateljem potrdil. Drugi nivo pa je v omrežje povezani izdajatelj potrdil. Za oba je potrebno zagotoviti maksimalno stopnjo varovanja.

Načrt za uvedbo mora zagotoviti ustrezno odzivnost sistema in dovolj redundance, da se doseže visok nivo odpornosti na napake. Odzivnost zagotovimo z visoko procesorsko močjo in z ustreznimi omrežnimi zmogljivostmi. Za korensko domeno imamo tri domenske nadzornike, dva sta DNS strežnika. Domenski nadzorniki posameznih domen članic so ravno tako replicirani. Strojna oprema strežnikov je podrobno predpisana in določena glede na velikost članice. Zaradi gospodarnosti izkoriščenosti virov je dovoljen določen nivo virtualizacije. Natančno je določeno tudi poimenovanje strežnikov, tako da je že iz imena razvidno ali gre za navidezen ali resničen stroj, kakšna je njegova vloga ter kje se nahaja.

5. SKLEP

V času pisanja tega članka so vzpostavljeni strežniki za skupni imenik na več kot devetih desetinah članic. Na več kot polovici članic je končana migracija uporabniških računov. Vzpostavljena je študentska domena, izdelana pa je tudi lastna rešitev za povezavo in usklajevanje z imenikom OpenLDAP. Preden lahko zares govorimo o delujočem sistemu za upravljanje z digitalnimi identitetami, je potrebno še vzpostaviti strežnik ILM za usklajevanje identitet. Naslednji korak pa je že vzpostavitev certifikatne agencije in izdaja digitalnih potrdil vsem zaposlenim in študentom. Z organizacijskega vidika je nujno potreben element sistema tudi podpora uporabnikom (t.i. helpdesk) ter priprava navodil za skrbnike sistema po članicah. Vzporedno se bo vzpostavil sistem za nadzor sistema, ki bo omogočal spremljanje varnostnih dogodkov, razpoložljivosti sistema in zanesljivosti storitev.

Podobno kot pri uvajanju klasičnih informacijskih rešitev se tudi pri uvajanju sistema za upravljanje z identitetami ponekod srečujemo z nezaupanjem predlagani rešitvi in z miselnostjo, da je delo po starem popolnoma v redu. Vendar pa projektni tim, čeprav je na obzorju še veliko dela, z optimizmom gleda v prihodnost.

6. VIRI IN LITERATURA

[1] A.Pfitzmann et.al. : Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology. Dosegljivo na http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.26.pdf. 2006.

[2] M. Casassa Mont, P. Bramhall, J. Pato: On Adaptive Identity Management: The Next Generation of Identity Management Technologies. HP technical report, 2003. Dosegljivo na www.hpl.hp.com/ techreports/2003/ HPL-2003-149.html.

[3] D. A. Buell, R. Sandhu: Identity Management. IEEE Internet Computing, dec. 2003.

[4] S. Subenthiran, K. Sandrasegaran, R. Shalak. Requirements for identity management in next generation networks. Proc. 6th Int. Conf. Advanced Communication Technology ICACT 2004. IEEE 2004. Dosegljivo na http://ieeexplore.ieee.org/iel5/9073/28786/01292845.pdf.

[5] S.S.Y. Shim, G. Bhalla, V. Pendyala: Federated Identity Management. IEEE Computer, December 2005.

[6] A. Bhargav-Spantzel, A. C. Squicciarini, E. Bertino: Trust Negotiation in Identity Management. IEEE Security &Privacy, April 2007.

[7] LADAVA, Matjaž, ZDOVC, Peter, JAGODIC, Anton, METELKO, Damir, OREHEK, Ivan, ČEPIN, Peter, GROM, Matej, GOVEJŠEK, Andrej, PANČUR, Matjaž, KREVL, Andrej, CIGLARIČ, Mojca. Načrt za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet. Ljubljana: Fakulteta za računalništvo in informatiko, 2007.

[8] R.Novak, G.Cotman, A.Krevl, M.Pančur, A.Jagodic: Priporočilo članicam Univerze – omrežje METULJ, Iskrasistemi, FRI, UL, Julij 2007

[9] M. Pančur, A. Jagodic, A. Govejšek, A. Budja, J.Zabukovec, A. Krevl: Poimenovanje objektov v AD, Microsoft, FRI, UL, Januar 2008

[10] M. Pančur, A. Jagodic, A. Govejšek, A. Budja, A. Krevl: Ustvarjanje študentskih digitalnih identitet, Microsoft, FRI, UL, Oktober 2007

[11] M. Pančur, A. Jagodic, A. Govejšek, A. Krevl: Ustvarjanje digitalnih identitet zaposlenih, FRI, UL, December 2007

Informacijska družba: multidisciplinarni pogledi

Information Society: Multidisciplinary Approaches

Informacijska družb: multidisciplinarni pogledi – Information Society: multidisciplinary approaches
Uroš Pinterič, Urša Šinkovec (ur.)

Recenzenta:
Dr. Janez Povh
Dr. Blaž Rodič

Fakulteta za uporabne družbene študije

Naklada: 200 izvodov
Naslovnica in prelom: Artline d.o.o.
Tisk: Littera Picta

Izzid monografije je sofinancirala Agencija za raziskovalno dejavnost Republike Slovenije

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

659.2:004:316.42(082)

INFORMACIJSKA družba : multidisciplinarni pogledi = Information
society : multidisciplinary approaches / Uroš Pinterič, Urša
Šinkovec (ur./eds.). - Nova Gorica : Fakulteta za uporabne družbene
študije, 2008

ISBN 978-961-6718-08-0
1. Vzp. stv. nasl. 2. Pinterič, Uroš
240553216

STRATEGIJA UPRAVLJANJA Z DIGITALNIMI IDENTITETAMI

dr. Mojca Ciglarič[1], Andrej Krevl[2], dr. Matjaž Pančur[3]

Povzetek

Celostna strategija upravljanja z digitalnimi identitetami zlasti v veliki organizaciji mora oziroma naj bi služila kot vodilo za izvedbo posameznih namenskih projektov ali faz tistih projektov, za katere v organizaciji obstaja potreba za zagotavljanje strateško skladnega obravnavanja identitete. Končni cilj je, da bi bili s strategijo skladni vsi posamezni deli porazdeljenega informacijskega sistema. Strategijo upravljanja z digitalnimi identitetami vedno sestavlja več vsebinsko zaokroženih sestavnih delov, temeljna vsebinska področja pa so upravljanje z gesli, nadzor dostopa, osrednji imenik in po potrebi še nekatera druga, specifična področja.

Glavne prednosti enotnega upravljanja z identitetami so zmanjšanje časa, potrebnega za administracijo uporabnikov, manj klicev na uporabniško podporo, večja varnost sistema kot celote. Kljub vsemu največjo grožnjo sistemski varnosti predstavlja človeški faktor, na primer uporabnik, ki zapusti svojo delovno postajo in se ob tem ne odjavi iz sistema. Vsakdo iz nje lahko namreč takoj dostopa do vseh podatkov in drugih virov, do katerih je upravičen ta uporabnik. Kljub tej slabosti pa je poleg učinkovitejše administracije največja priložnost, ki jo lahko izkoristi organizacija ob uvedbi enotnega upravljanja z identitetami, ravno dvig varnostnega nivoja celotnega sistema in varnostne ozaveščenosti uporabnikov sistema.

Uvod

Čeprav se kaže področje upravljanja z digitalnimi identitetami zlasti v zadnjem letu ali dveh vedno bolj aktualno, v literaturi ne najdemo večjega števila tehtnih del s tega področja. Po eni strani nas izdelovalci in prodajalci sistemov za

---

[1] Doc. Dr. Mojca Ciglarič je doktorirala leta 2003 na UL, Fakulteti za računalništvo in informatiko, na področju računalniških komunikacij. Zaposlena je na UL FRI, pedagoško deluje tudi na FUDŠ, raziskovalno in strokovno pa deluje zlasti na področju porazdeljenih sistemov.

[2] As. Andrej Krevl je diplomiral iz računalništva in informatike na UL FRI, kjer je zaposlen kot asistent in zaključuje magistrski študij računalništva, raziskovalno in strokovno pa se ukvarja z vsemi vidiki sistemske infrastrukture.

[3] Dr. Matjaž Pančur je doktoriral leta 2005 na UL FRI na področju metodologij razvoja programske opreme. Raziskovalno in strokovno se ukvarja z razvojem programske opreme, pa tudi s komunikacijami in porazdeljenimi sistemi.

upravljanje z digitalnimi identitetami zasipajo s komercialnim materialom in na pol tehničnimi navodili za vzpostavljanje in konfiguriranje sistema, po drugi pa manjka globljega razumevanja in vodil, na podlagi katerih se odločiti za tovrsten sistem in kako ga uporabljati v skladu z začrtano strategijo.

Med ponudniki sistemov za upravljanje z digitalnimi identitetami lahko srečamo najbolj znane akterje trga programske opreme: Microsoft (ILM - Identity Lifecycle Management), pa seveda Oracle, IBM, Sun Microsystems, HP..., prav tako pa tudi številna vsaj pri nas neznana podjetja, kot na primer naključno izbrani Avatier [8].

Med teoretičnimi deli naj izpostavim tri. V dokumentu [5] ki se razvija in posodablja že skoraj deste let in je bil že mnogokrat objavljen in citiran, avtor zastavi podrobno taksonomijo pojmov na področju anonimnosti uporabnika, vključno s pojmi identiteta, psevdonim in »neopazljivost« (unobservability). V novejših različicah dokumenta je pojem identitete podrobneje razdelan in se razširi tudi na področje upravljanja z identitetami in posledično sistemov za upravljanje z identitetami.

V članku [4] avtorji zasledujejo koncept multilateralne varnosti komunikacije, torej take izvedbe varne komunikacije, ki zagotavlja varnost ne le »svojim« uporabnikom, ampak vsem udeležencem komunikacije. Izkaže se, da je najboljša izvedba večstranske varnosti ravno tista, ki vključuje uporabo sistema za upravljanje z digitalnimi identitetami. Na nekaj pogostih primerih avtorji izpeljejo tudi obsežen seznam zahtev, ki jih mora podpirati upravitelj digitalnih identitet ter predlagajo možne načine integracije obeh sistemov.

V članku [3] pa avtorji opisujejo tehnologije za omogočanje zasebnosti kot odgovor na današnje legalne in tudi družbena pričakovanja in zahteve povedno višji stopnji zasebnosti. Ker tehnologije same po sebi kot orodje niso praktične, avtorji predlagajo njihovo uporabo in vključevanje v sisteme za upravljanje z digitalnimi identitetami. Pri tem izpostavijo šibke točke današnjih sistemov za upravljanje z digitalnimi identitetami in predlagajo izboljšan koncept njihove izgradnje.

Kot zanimivo množico dokumentov s področja upravljanja z identitetami navedimo še spletno stran projekta upravljanja z digitalnimi identitetami ameriške univerze Santa Cruz [1], zlasti dokument, ki opisuje strategijo celotnega sistema in nam je bil v oporo tudi pri pisanju tega članka. Podobno strategijo opisuje tudi dokument [2], ki je sicer starejši in nosi še naziv osnutek, vendar ravno tako zanimivo osvetljuje nekatere vidike upravljanja z digitalnimi identitetami.

Namen tega članka je kratko, a vendar informativno opisati področje upravljanja z digitalnimi identitetami, definirati najpomembnejše pojme, opisati osnoven gradnike sistemov za upravljanje z digitalnimi identitetami in cilje njihovega uvajanja ter nazadnje začrtati okvir strategije takega sistema, ki jo bomo ilustrirali tudi s konkretnimi izkušnjami, pridobljenimi na primeru univerze v Ljubljani.

Osnovni pojmi

Po [5] je identiteta osebka tista množica atributov, ki ga identificira znotraj neke množice osebkov. Ker so množice osebkov lahko zelo različne, tudi ta množica atributov ni enaka v vsaki množici osebkov. Lahko torej trdimo, da osebek nima ene unikatne identitete, ampak lahko celo množico identitet. Vrednosti atributov in tudi sami atributi se lahko sčasoma spreminjajo, torej se nujno spreminjajo tudi identitete.

Vloga (ang. role) je množica akcij ali tudi pričakovano obnašanje osebka v določenih okoliščinah. Delna identiteta osebka, ki ji lahko ustreza psevdonim osebka (oziroma eden od psevdonimov), pa je tista podmnožica atributov celotne identitete, ki predstavlja ta osebek v določeni vlogi.

Digitalna identiteta osebka je množica tistih atributov osebka, ki so shranjeni, povezani in dosegljivi s pomočjo računalniške tehnologije.

Upravljanje z identitetami s pomočjo tehnologije se v najširšem smislu nanaša na načrtovanje in upravljanje podatkov, ki sestavljajo digitalno identiteto. Sistem za upravljanje z digitalnimi identitetami je infrastruktura, kjer se usklajeno uporabljajo različne aplikacije in orodja (odjemalska ali strežniška) za upravljanje z identitetami. Takšen sistem omogoča razpoznavanje različnih vrst komunikacije in različnih situacij ter jih vrednoti glede na pomen, funkcionalnost, pa tudi tveganje za varnost in zasebnost. Glede na to sistem opredeljuje, identitetam dodeljuje in uporablja ustrezne vloge.

S svojo digitalno identiteto se uporabnik prvič sreča ob prijavi na računalnik. Čeprav preverjanje zgolj uporabniškega imena in gesla samo po sebi ni težko opravilo, pa so pravi sistemi za upravljanje digitalnih identitet kompleksni in jih uspešno uporabljajo le redke organizacije.

Primer:

Informacijski sistem Univerze v Ljubljani ima več kot 70.000 uporabnikov (skupno število zaposlenih in študentov), razpršenih po članicah in na upravi Univerze. Ti uporabniki vsakodnevno dostopajo do informacijskega sistema in

zahtevajo dostop do različnih storitev v okviru svoje fakultete, univerze, kot tudi do storitev, ki jih nudijo partnerske inštitucije.

Zakaj upravljanje z digitalnimi identitetami?

314

Splošni cilji uvedbe upravljanja z digitalnimi identitetam so naslednji:

1. **Udobje in boljša storitev za uporabnika**: to dvoje se uresničuje s pomočjo zmanjšanja števila različnih identitet uporabnika (različna uporabniška imena in gesla za različne aplikacije in sisteme) – v končni fazi se uresniči enkratno prijavljanje z eno samo identiteto (single sign-on). Ena sama identiteta pa pomeni tudi eno samo mesto za vzdrževanje podatkov o dostopu v različne sisteme in o kontaktnih ter drugih podatkih uporabnika. Za uresničenje le tega je potrebna ustrezna povezava s končnimi (zalednimi) aplikacijami in vmesnik za končnega uporabnika, če mu dovolimo, da tudi sam vnaša in spreminja svoje podatke.
2. **Podpora e-poslovanju:** zaledni sistemi in aplikacije lahko transparentno izvajajo avtorizacijo in avtentikacijo uporabnikov, uporabniki pa lahko (celo znotraj ene transakcije) dostopajo do podatkov in storitev, ki jih sicer nudijo različni zaledni sistemi in aplikacije. Tako lahko množica porazdeljenih sistemov, aplikacij in storitev deluje kot celovit, integriran porazdeljen sistem.
3. **Osrednji imenik:** imenik je središčna točka vsakega sistema za upravljanje z digitalnimi identitetami in predstavlja povezavo s podatki v zvezi z identitetami v zalednih sistemih. S svojimi podatki ponazarja tudi posnetek organizacijske strukture, obenem pa zaradi poenotenega upravljanja z identiteto na enem mestu znižuje stroške vodenja in povezovanja imenikov.
4. **Organizacijska struktura**: z ustreznim dodeljevanjem vlog uporabnikom sistema se ustvarja posnetek organizacijske strukture in konsistentno dodeljevanje pravic in omejitev uporabnikom z enakimi vlogami. Uporabnike se lahko obravnava bodisi skupinsko bodisi individualno, s tem se tudi olajšuje delo administratorjem.
5. **Delovni tokovi**: vzpostavljen sistem upravljanja z digitalnimi identitetami omogoča informacijsko podporo izvajanja delovnih tokov (workflow) poslovnega procesa (tudi prek več zalednih sistemov in aplikacij), v katerih uporabniki sodelujejo na podlagi svojih dodeljenih vlog. Okolje za izvajanje podatkovnih tokov ali upravljanje poslovnih

procesov je lahko ločeno od sistema za upravljanje digitalnih identitet – z njim je lahko povezano na enak način kot katerikoli drug zaledni sistem.

6. **Zagotavljanje in nadzor dostopa do virov** (provisioning): Uporabnik ob prijavi avtomatsko dobi dostop do tistih virov, aplikacij in sistemov, ki pripadajo njemu dodeljenim vlogam. Obenem ima onemogočen dostop do tistih virov, aplikacij in podsistemov, ki njemu dodeljenim vlogam ne pripadajo.
7. **Varnost in zasebnost:** Zmanjša ali izniči se potreba po pomnjenju, varnem hranjenju ali zapisovanju številnih uporabniških imen in gesel za dostop do različnih sistemov. Prav tako se zmanjša ali izniči potreba po skupinskih geslih, ki so še zlasti varnostno problematična.

V članku bomo naštete cilje podrobno razdelali in podali ogrodje strategije, ki zajema vsa ciljna področja upravljanja z digitalnimi identitetami in zasleduje njihovo izpolnitev. Teorijo bomo popestrili s konkretnimi primeri tovrstne strategije, izdelane za Univerzo v Ljubljani (v nadaljevanju UL), zato v nadaljevanju najprej predstavimo nekatere posebnosti univerzitetnega okolja.

Digitalne identitete v univerzitetnem okolju

Informacijski sistemi Univerze v Ljubljani so razpršeni po članicah (fakultetah, oddelkih, pisarnah...), ki imajo poleg maloštevilnih skupnih aplikacij specifičen nabor lastnih aplikacij, med katerimi nekatere niso združljive z aplikacijami drugih članic in uporabljajo svoje avtentikacijske in avtorizacijske sisteme.

S postopnim uvajanjem bolonjskega študija se povečuje mobilnost študentov in profesorjev, ki potrebujejo dostop do univerzitetne informacijsko komunikacijske infrastrukture tudi na drugih lokacijah, ne le na svoji matični, zato se število njihovih digitalnih identitet še povečuje kljub dejstvu, da tehnologija omogoča, da bi vsak posameznik tudi v velikem in kompleksnem sistemu imel le eno digitalno identiteto.

Dolgoročni cilj Univerze v Ljubljani je vzpostavitev centralnega sistema za upravljanje digitalnih identitet za celotno Univerzo v Ljubljani – za vse zaposlene in tudi vse študente. Ta sistem bo podatke o identitetah zajemal iz obstoječih podatkovnih baz, in sicer glavnino iz postopka vpisa na univerzo in iz kadrovske evidence. Upravljal bo z identitetami za obstoječe storitve informacijskega sistema Univerze, hkrati pa bo omogočil razvoj novih storitev, kot so enotna elektronska pošta za študente, dopisni seznami, skupni koledarji in centralni imenik. Poenostavil bo administracijo digitalnih identitet in razbremenil

skrbnike informacijskih sistemov na fakultetah, obenem pa ustrezno poskrbe
varnost.

Okviri strategije za upravljanje z digitalnimi identitetami

316 Vsi zaposleni in glede na naravo organizacije lahko tudi zunanji poslovn
partnerji morajo imeti možnost preprostega, a vendar varnega dostopa do viro
informacijskega sistema in do njegovih storitev od koderkoli prek interneta
zahteva je v času globalizacije in vedno večje mobilnosti pogosto imperativ
izgradnjo odprte, a varne informacijske infrastrukture, vzpostavitev učinkovit
in razširljivih procesov upravljanja dostopa do virov in uveljavljanje striktni
pravil in zahtev glede dostopa do organizacijskih informacijskih virov in storitev
Čeprav bi vzpostavljen sistem organizacija navadno potrebovala že danes al
celo včeraj, se navadno vzpostavljala postopno, v daljšem časovnem obdobju
kot zaporedje več ločenih informacijskih projektov z manjšimi, a jasno
določenimi cilji. Na UL so to na primer projekt zagotavljanja enotnih
elektronskih naslovov za vse študente, projekt vzpostavitve univerzitetne
certifikatne agencije in podobni.

Iz do sedaj napisanega je jasno, da so sistemi za upravljanje z identitetami velik
in kompleksni. Vsi ti delni, manjši projekti morajo upoštevati enotno strategijo
in enotne varnostne politike, ki v praksi pogosto še niso napisane. Rezultati
morajo zagotavljati morali razširljivost na mnogo, celo več desettisoč
uporabnikov in nuditi visoko stopnjo razpoložljivosti, kar za seboj potegne tudi
redundančno zasnovano infrastrukturo in primerno organizacijo dela v službi za
informacijsko infrastrukturo in podporo uporabnikom.

Zaradi omogočanja povezljivosti z informacijskimi sistemi drugih organizacij in
inštitucij je dobro, da sistem za upravljanje z digitalnimi identitetami omogoča
tudi združevanje (ang. federation) identifikacijskih podatkov iz različnih
sistemov za upravljanje z digitalnimi identitetami po principih danes splošno
sprejetih standardnih tehnologij s tega področja. Ravno tako pa ne smemo
pozabiti na varnostne standarde (zlasti ISO 27001:2005) in dobre prakse
upravljanja informacijskih procesov (npr. ITIL), saj saj bo le tako sistem lahko
vzpostavil primerno mero zaupanja s strani uporabnikov sistema

Primer:

*Izzivi, s katerimi se pri uvajanju sistema za upravljanje z digitalnimi identitetami
srečuje UL, so številni. Predvideno končno število uporabnikov je 70.000 (tu niso
všteti »alumni«, torej bivši študentje). Zaželjen ciljni razred razpoložljivosti
sistema je "pet devetk", torej da sistem deluje 99.999% časa (dovoljeno je*

približno 5 minut izpada v enem letu). Potrebna bodo velika vlaganja v sistemsko infrastrukturo in vzpostavitev podpore uporabnikom – tako imenovanega help desk-a. Ker se v sistemu za upravljanje z digitalnimi identitetami hranijo tudi osebni podatki, je potrebno pri vzpostavljanju upoštevati Zakon o varovanju osebnih podatkov in v skladu z njim še več pozornosti posvetiti varnemu hranjenju podatkov in onemogočanju nepooblaščenega dostopa. Prav tako je želja, da bi se omogočila povezljivost z nekaterimi zunanjimi inštitucijami, na primer da bi bilo možno elektronsko prijavljanje na razpise ARRS, zato je nujno zagotoviti združljivost z drugimi sistemi.

V nadaljevanju bomo navedli nekaj najznačilnejših vsebinskih področij, ki se jih mora dotakniti strategija upravljanja z identitetami za vsako organizacijo.

Koliko identitet na osebo?

Večina organizacij teži k magični frazi Single Sign-On (SSO) oziroma k cilju ena oseba – ena identiteta. Vendar pa je, sploh v velikih organizacijah, kjer se uporablja večje število imenikov in množica različnih aplikacij, to težko doseči. Kot vmesni cilj se zato uveljavlja kompromisni Reduced Sign-On, torej zmanjšano število identitet uporabnika na nek razumni, še znosni minimum. V fazi oblikovanja strategije mora organizacija presoditi, ali bo sposobna izvesti prehod na enotno identiteto takoj ali pa bo ta prehod postopen. Če bo prehod postopen, je potrebno tudi opredeliti faze prehoda in določiti pravila oziroma robne pogoje za vzpostavitev oziroma ohranitev vsake naslednje identitete uporabnika razen prve (primer: uporabniki, ki uporabljajo neko aplikacijo s specifičnimi tehnološkimi zahtevami, imajo za vstop v to aplikacijo ločeno identiteto).

Ustvarjanje nove digitalne identitete

Novo digitalno identiteto v organizaciji navadno ustvarimo ob vsaki novi zaposlitvi. Takrat se ustvari ustrezno uporabniško ime in začetno geslo, strategija pa mora opredeljevati uporabnikovo ravnanje z geslom, na primer kako pogosto ga mora le ta menjati, kako dolgo in kako kompleksno mora biti... Če se digitalne identitete ustvarjajo avtomatsko, strategija opredeljuje tudi pravila aktivacije digitalne identitete in neke minimalne uporabniške pravice, ki jih dobi sveže aktivirani uporabnik. Dodeljevanje nadaljnjih vlog in pravic je omogočeno skrbnikom prek sistema za upravljanje z digitalnimi identitetami, prav tako kot tudi odvzemanje vlog (ang. provisioning in deprovisioning).

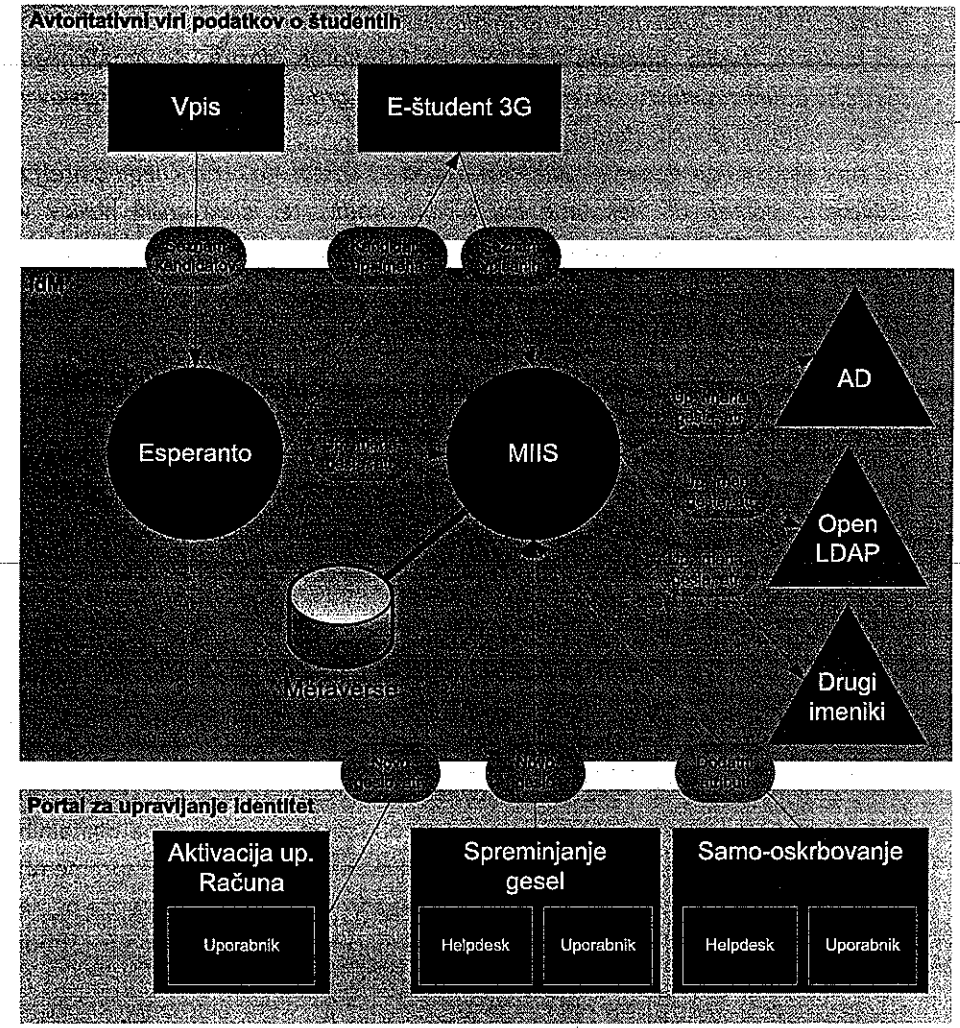
Primer:

Študentje UL prejmejo svojo digitalno identiteto ob vpisu na fakulteto. Za vsakega študenta se ustvari uporabniško ime in naključno začetno geslo. Če se študent strinja s pogoji uporabe informacijskih storitev UL, lahko s pomočjo teh podatkov aktivira (omogoči) svoje uporabniško ime, si nastavi svoje geslo in (če to želi) dopolni podatke v svojem profilu. Ob prvi aktivaciji digitalne identitete so uporabniške pravice minimalne. Seveda se potrebe za dostop do informacijskih virov UL v toku študijskega procesa spreminjajo, zato omogoča sistem za upravljanje digitalnih identitet dodeljevanje in odvzemanje vlog uporabnikom. Skrbniki sistema na članicah lahko dodeljujejo vloge za dostop do računalniških učilnic, datotečnih virov, tiskalnikov, ipd. Na drugi strani pa se tudi nabor informacijskih storitev, ki jih nudi informacijska služba UL, povečuje, s tem pa se povečuje tudi število vlog, ki pripadajo posameznem študentu. Zato imajo tudi skrbniki sistema na UL možnost dodajanja in odvzemanja vlog študentom. Omogočeno je tudi dodajanje začasnih vlog, kot je na primer sodelovanje na različnih projektih Ob zaključku študija ostane uporabniško ime aktivno, le da se ga uvrsti v program Alumni, odvzame pa se večina vlog, ki omogočajo dostop do informacijskih virov UL.

Zaposlenim se ustvari digitalna identiteta takoj ob nastopu dela. Sistem za upravljanje digitalnih identitet nenehno pregleduje spremembe v kadrovskih evidencah in na podlagi novega zapisa v kadrovski evidenci ustvari novo digitalno identiteto za zaposlenega. Kljub temu, da zaposleni nastopajo v drugačnih vlogah kot študentje, je upravljanje z vlogami rešeno na podoben način. Vloge, ki omejujejo dostop do virov na posameznih fakultetah, upravljajo lokalni skrbniki, globalne vloge za dostop do informacijskih virov UL pa upravljajo skrbniki v osrednji informacijski službi UL.

O digitalni identiteti smo do sedaj govorili kot o kombinaciji uporabniškega imena in gesla, vendar pa sistemi za upravljanje digitalnih identitet omogočajo tudi močnejše načine avtentikacije uporabnikov. UL na primer načrtuje za vse uporabnike uporabo digitalnih potrdil.

Slika 1: Zgradba sistema UL in postopek ustvarjanja ali spreminjanja identitete



319

Minimalen nabor pravic

Ob kreiranju nove digitalne identitete le ta dobi nek minimalen nabor pravic. Strategija mora opredeljevati, kakšen konkretno je ta nabor. Navadno obsega vsaj elektronski naslov v domeni organizacije in dostop do poštnega strežnika in dostop do intraneta, lahko pa tudi dostop do osnovnih aplikacijskih virov, datotečnih strežnikov, portala za podporo skupinskemu delu in podobno.

Primer:

Minimalne pravice digitalnih identitet na UL se razlikujejo glede na vlogo posameznika. Pri študentih obsega minimalen nabor pravic: dostop do aplikacije za podporo študija, uporaba Info točk na fakultetah, dostop do brezžičnega omrežja Eduroam, dostop do nekaterih knjižničnih gradiv ter elektronski naslov v univerzitetni študentski domeni.

320

Za zaposlene pa obsega minimalen nabor pravic: dostop do brezžičnega omrežja Eduroam, dostop do nekaterih knjižničnih gradiv, ter elektronski naslov v univerzitetni ali fakultetni domeni.

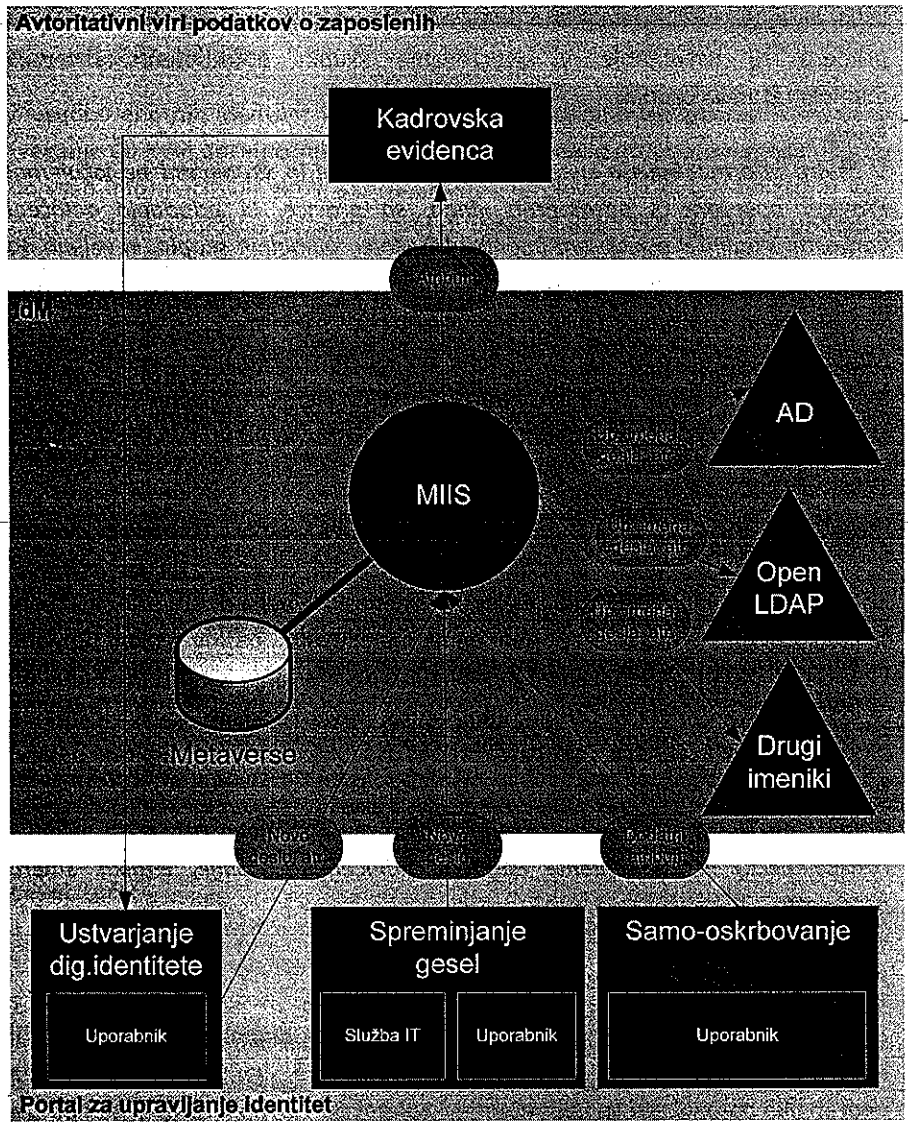
Dodajanje novih vlog ali pravic

Nove vloge in s tem pravice za dostop do informacijskih virov se dodajajo v skladu s potrebami delovnega procesa in z delovnimi nalogami posameznika. Dodajanje vlog je pogosto ročno in za to poskrbi skrbnik sistema, nekatere spremembe pa so vendarle lahko tudi avtomatizirane. Če se na primer zaposleni napreduje na boljše delovno mesto, se po spremembi zapisa v kadrovski podatkovni bazi lahko sprememba avtomatsko prenese v sistem za upravljanje z digitalnimi identitetami, ki ustrezno odreagira z dodajanjem nove vloge.

Primer:

Nove vloge zaposlenega UL se dodelijo na podlagi spremembe delovnih nalog, zaradi sodelovanja na projektu, zaradi dodatnih pedagoških obremenitev na drugih članicah, ipd. Vloge študentov se lahko spreminjajo ob vpisu v knjižnico, ob pridobitvi novega statusa (vpis v nov študijski program, zaključek študija), ob vključevanju v projektne skupine in podobno. Sistem za upravljanje digitalnih identitet omogoča nekaj avtomatskega dodeljevanja vlog na podlagi sprememb v podatkovnih bazah študijske informatike in kadrovske evidence. Seveda pa ne moremo pričakovati popolnega avtomatizma, saj je dodeljevanje zaradi značilnosti posameznih zalednih sistemov to skoraj nemogoče.

Slika 2: usklajevanje identitet za zaposlene na UL.

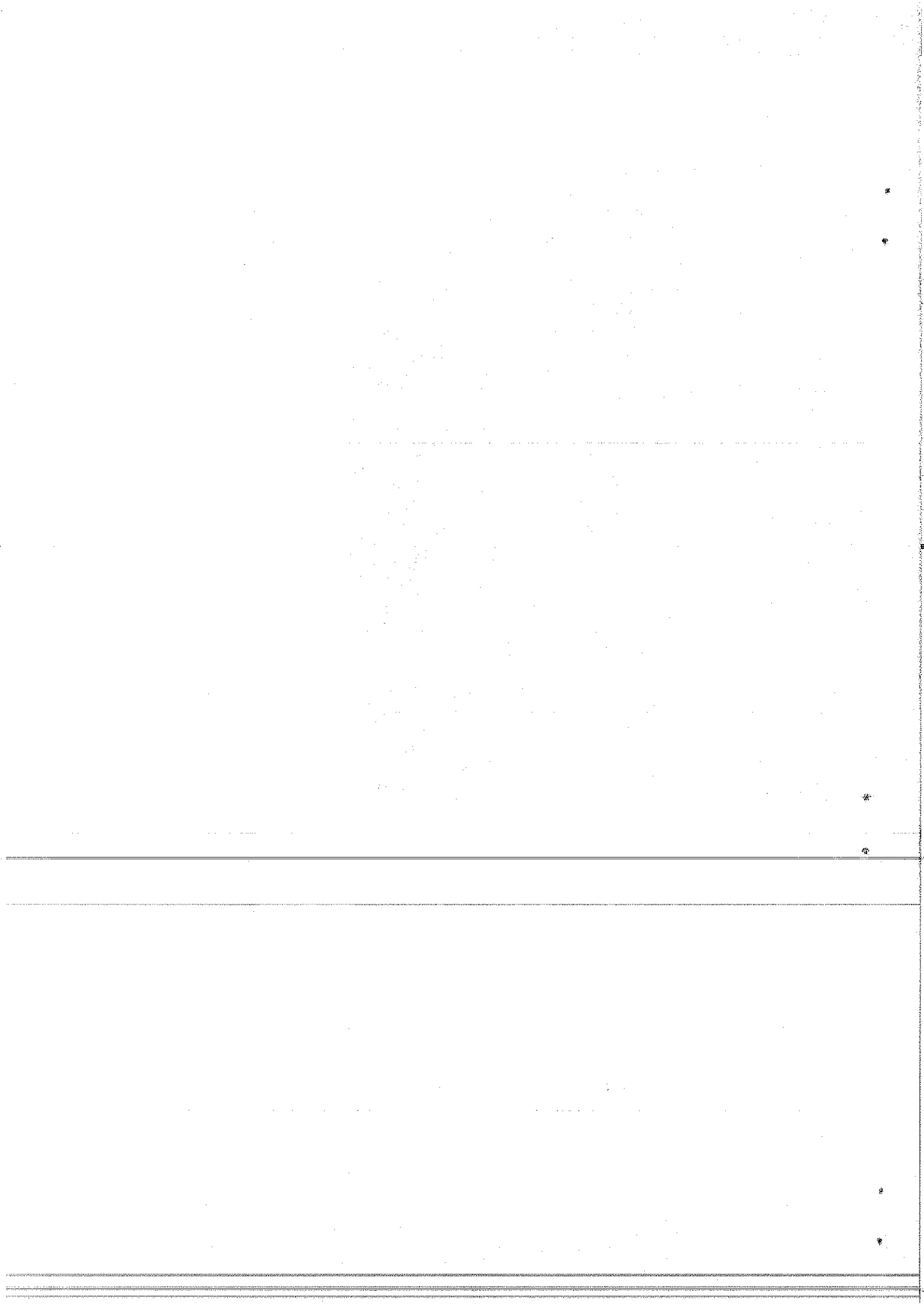


321

Uporabniške skupine, varnostne skupine

Uporabniške skupine olajšajo sistemsko administracijo in omogočajo preprosto zagotavljanje konsistentnosti pravic in omejitev. Pri ustvarjanju uporabniških skupin sta dovoljena dva pristopa.

Prvi pristop predstavlja ustvarjanje skupine tako, da se vsem članom dodeli enake vloge. Drugi pristop pa predstavlja ustvarjenje skupinskega objekta -



grupe (na primer e-poštnega naslova), kateremu opredelimo ustrezne pravice in/ali omejitve, in nato poljubno dodajanje uporabnikov v to skupino. V vsakem primeru za ustvarjanje in vzdrževanje skupin potrebujemo ustrezna administratorska orodja.

322 *Primer:*

V okviru informacijskega sistema UL med vlogami in skupinami ne ločujemo. Pravice, povezane s posamezno vlogo, so pravice, ki pripadajo določeni varnostni skupini v osrednjem imeniku UL. Poleg globalnih skupin, ki veljajo na nivoju celotnega imenika, vsaka fakulteta lahko ustvari lastne varnostne skupine, ki omogočajo dodeljevanje pravic do različnih virov.

Med globalnimi vlogami so tudi vloge, ki omogočajo aplikacijam avtentikacijo in avtorizacijo uporabnikov. Za avtomatizirano včlanjevanje uporabnikov v te vloge skrbi sistem za upravljanje digitalnih identitet, za ročno pa informacijska služba UL.

Elektronski naslovi

Kot za digitalne identitete tudi za elektronske naslove velja dobra praksa, da naj bi imel v organizaciji vsak zaposleni en sam elektronski naslov v njeni domeni. Elektronski naslov pa se ne sme uporabljati za dokazovanje identitete! To naj bo le eden od podatkov v profilu uporabnika. Naslove se, tako kot digitalne identitete, lahko razvršča v skupine, prav tako lahko obstajajo skupinski naslovi (distribucijski seznami).

Primer: na UL se oblikujejo poštni seznami za zaposlene (asistenti, učitelji, raziskovalci...) in za študente (študenti določenega študije, letnika, smeri, predmeta, ...).

Prijava v aplikacije in dostop do storitev

Zaželeni način prijave v zadnji fazi uvajanja sistema digitalnih identitet naj bi bila, kot že večkrat zapisano, enotna prijava (Single Sign-On oz. SSO). To za uporabnika pomeni, da se najprej prijavi spletni portal, povezan s sistemom za upravljanje z digitalnimi identitetami, nato pa se mu v druge aplikacije ni potrebno ponovno prijavljati, saj je že avtenticiran in ga torej sistem že pozna. Dokler enotna prijava ni tehnično ali organizacijsko izvedljiva (tudi npr. zaradi tehnologije obstoječih aplikacij), je sprejemljiva tudi neposredna prijava v ciljno aplikacijo, ki pa naj za avtentikacijo uporablja podatke iz osrednjega imeniškega sistema (princip "campus-wide login"). Pri tem principu uporabnik še vedno

uporablja zgolj eno uporabniško ime in geslo za dostop do različnih storitev, vendar pa ga mora vnašati na različnih mestih (v različnih aplikacijah).

Preprečevanje zlorab

Z uvedbo enotnih identitet in centralnega imenika se povečuje tudi varnostno tveganje ob kraji posameznikove identitete, saj ena identiteta omogoča dostop do vseh informacijskih virov UL. Na sistemskem nivoju je potrebno storiti vse, da identitete ni možno zlorabiti, torej ni možno (ali pa je zelo težko) uporabiti identiteto nekoga drugega. Zloraba je na UL lahko kritična na primer pri izpitih, manj kritična pa v primeru, ko lastnik identitete to prostovoljno "posodi" za dostop do svojih virov. Uporabnike je potrebno konstantno izobraževati in varnostno ozaveščati, saj se morajo zavedati, da ima tudi »neškodljivo posojanje« identitet, lahko za posledico resno ogrožanje posameznikove varnosti.

Potek projekta vzpostavljanja sistema za upravljanje digitalnih identitet na UL

Vzpostavitev sistema za upravljanje digitalnih identitet na nivoju Univerze je velik organizacijskih in tehnični izziv tudi zaradi heterogenosti infrastrukture, s katero je potrebno zagotoviti povezljivost, zaradi velike množice uporabnikov ter značilnosti njihove organiziranosti. Menimo, da bodo tudi zaradi tega izkušnje, pridobljene na projektu, zanimive za širšo javnost v Sloveniji, pa tudi v tujini.

Sama izvedba projekta je načrtovana v več fazah, ki jih vsebinsko lahko delimo v devet točk:

1. Izdelava analize, primerjava in izbira najprimernejšega sistema za upravljanje digitalnih identitet
2. Izdelava načrta za vpeljavo, organizacijo in vodenje sistema za upravljanje digitalnih identitet
3. Priprava strategije prehoda na integriran sistem za upravljanje digitalnih identitet, celovito zaščito in varovanje identitete
4. Priprava ITIL procesov za upravljanje z digitalnimi identitetami
5. Vzpostavitev centralnega imenika na upravi Univerze in povezovanje z obstoječimi sistemi (Vpis, Kadrovska evidenca...)
6. Pilotna vključitev ene manjše akademije in ene večje fakultete v sistem za upravljanje z digitalnimi identitetami
7. Testiranje delovanja in odpravljanje morebitnih napak

8. Postopna vključitev preostalih članic v sistem za upravljanje z digitalnimi identitetami.
9. Vzpostavitev univerzitetne certifikatne agencije

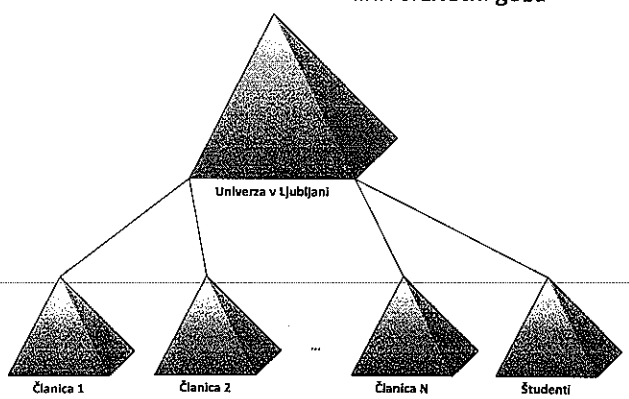
Arhitektura bodoče rešitve sestoji iz treh ključnih delov: osrednjega aktivnega imenika, sistema za sinhronizacijo podatkov o identitetah z zalednimi sistemi in sistema za upravljanje z digitalnimi potrdili. Ključna aktivnost v začetnih fazah projekta pa je bil razvoj načrta za uvedbo sistema. V njem so bile postavljene zahteve po ustrezni odzivnosti (razpoložljivost) in odpornosti na napake, ovrednotene so infrastrukturne zahteve – računalniki ter ustrezna programska in strojna oprema, standardi poimenovanja in podobno. Načrt zagotavlja, da se bodo imeniški podatki pravilno replicirali po sistemu in bodo zato vedno na voljo uporabnikom. Prilagojen je omrežni topologiji in obstoječi komunikacijski infrastrukturi UL, zato zagotavlja tudi ustrezno odzivnost in robustnost.

Naslednja ključna aktivnost je bila priprava strategije prehoda na integriran sistem za upravljanje digitalnih identitet, ki vključuje tudi celovito zaščito in varovanje identitete. Strategija zajema naslednja področja:

a) Poimenovanje objektov v centralnem imeniku
b) Migracija digitalnih identitet zaposlenih iz obstoječih imenikov v nov centralni imenik
c) Ustvarjanje in upravljanje digitalnih identitet za študente UL
d) Ustvarjanje in upravljanje digitalnih identitet za zaposlene na UL
e) Preslikava in usklajevanje atributov med imenikom in zalednimi sistemi
f) Priporočila za razvoj novih aplikacij

V času pisanja tega prispevka je osrednji imenik že vzpostavljen, velikost podatkovne baze je ocenjena na okrog 15 GB podatkov, uvaja pa se prva nova aplikacija, ki bo uporabljala avtentikacijo prek njega.

Slika 3: Struktura imenika UL – univerzitetni gozd



Pred začetkom sinhronizacije sistemov je bilo treba vzpostaviti aktivni imenik ter ustrezne domenske strežnike. Določiti je bilo treba tudi vsebinska pravila igre – kaj, kako, kdaj usklajevati. Namen sinhronizacije je nadzorovano pretakanje in usklajevanje podatkov o digitalnih identitetah med različnimi zalednimi sistemi in osrednjim aktivnim imenikom.

Tretja komponenta sistema za upravljanje z digitalnimi identitetami je osnovna arhitektura strežnikov za izdajo digitalnih potrdil. Digitalna potrdila omogočajo napredne varnostne scenarije v omrežju Univerze. Primeri takšnih scenarijev so v današnjem nevarnem internetu že samoumevni - denimo varna prijava na računalnike v omrežju, uporaba pametnih kartic, ki identificirajo uporabnike pri interakciji z različnimi sistemi, izdaja digitalnih potrdil za strežnike znotraj omrežja in podobno. Arhitektura rešitve predvideva vzpostvitev dvonivojske certifikatne avtoritete: prvi nivo predstavlja samostojni korenski strežnik, ki ni povezan v omrežje in izdaja digitalna potrdila v omrežje povezanim strežnikom - izdajateljem potrdil. Drugi nivo pa je v omrežje povezani izdajatelj potrdil. Za oba je potrebno zagotoviti maksimalno stopnjo varovanja.

Načrt za uvedbo mora zagotoviti ustrezno odzivnost sistema in dovolj redundance, da se doseže visok nivo odpornosti na napake. Odzivnost zagotovimo z visoko procesorsko močjo in z ustreznimi omrežnimi zmogljivostmi. Za korensko domeno imamo tri domenske nadzornike, dva sta DNS strežnika. Domenski nadzorniki posameznih fakultetnih domen so ravno tako replicirani. Strojna oprema strežnikov je podrobno predpisana in določena glede na velikost članice, zaradi gospodarnosti izkoriščenosti virov pa je dovoljen tudi določen nivo virtualizacije.

Zaključek

Zgoraj naštete točke predstavljajo poglavitne vsebine, ki se pojavijo že ob uvajanju osrednjega imenika, vendar pa še zdaleč ne zajemajo celotne problematike uvajanja sistema za upravljanje z digitalnimi identitetami. Zaradi konsistentnosti polnjenja in uporabe sistema za upravljanje digitalnih identitet je potrebno na primer za vsak vsebinski sklop podatkov v zvezi z identitetami odgovoriti na nekaj ključnih vprašanj: kaj je avtoritativni vir podatkov za ta sklop? Kako poteka sinhronizacija z osrednjim imenikom in zalednimi sistemi? Kaj se zgodi ob spremembi podatka v avtoritativnem viru?

Univerza v Ljubljani se je s tovrstnimi problemi uspešno spopadla in kljub številnim nepredvidenim tehničnim in organizacijskim zapletom se projekt bliža

uspešnemu zaključku. Prav zato avtorji članka upamo in verjamemo, da bodo opisane izkušnje zanimivo in poučno branje za vse, ki se lotevajo podobnih projektov in morda ne vedo, na katerem koncu jabolka bi bilo vredno narediti prvi ugriz.

Viri in literatura:

UC Santa Cruz: Identity Management Project Documents, dosegljivo na http://its.ucsc.edu/idm/doc_index.php (julij 2007)

Identity Management Strategy draft v1.03, februar 2005, dosegljivo na http://www.e-strategy.ubc.ca/_shared/assests/IDMS-strategy-11932.pdf (julij 2008).

Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A. and Waidner, M.: Privacy-enhancing identity management, Information Security Technical Report, Volume 9, Issue 1, Elsevier Ltd., January-March 2004, pp. 35-44, doi:10.1016/S1363-4127(04)00014-7.

Clauß, S. and Köhntopp, M., 2001. Identity Management and Its Support of Multilateral Security, Computer Networks, vol. 37 (2001), *Special Issue on Electronic Business Systems*, Elsevier, North-Holland, pp. 205–219.

Pfitzmann, A., Hansen, M.: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v0.31 Feb. 15, 2008). Dosegljivo na http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Ciglarič, M., Krevl, A., Pančur, M.: Strategija upravljanja z digitalnimi identitetami na Univerzi v Ljubljani, različica 1.0, Univerza v Ljubljani, april 2008.

Krevl, A., Pančur, M., Ciglarič, M.: Uvajanje enotnega upravljanja z digitalnimi identitetami na univerzi v Ljubljani, Zbornik Dnevi slovenske informatike 2008, Portorož, April 2008.

Spletna stran Avatier; http://www.avatier.com (julij 2008).

Mojca Ciglarič

Building an Identity Management Strategy

Submitted to: Palgrave McMillan: European journal of information systems

ABSTRACT

In large organizations, integrated digital identity management strategy should offer guidance at accomplishing other target projects or project phases, related to digital identities of its employees or clients. The ultimate strategic goal is a consistent treatment of digital identities throughout all of the distributed information system(s) segments. The digital identity management strategy consists of several parts; among them are password management, access control, central directory management and others. The benefits of unified identity management are easier user administration, less helpdesk calls, higher system security level... Although from the security point of view, the users still represent the weakest link, the most important issue that an organization should benefit from when introducing unified identity management strategy is higher overall system security.

The paper overviews the area and suggests a content framework for the digital identity management strategy. The framework is illustrated with fragments from the real world case at University of Ljubljana with just over 70 000 users. At last, our IDMS system project is outlined and some experiences are briefly discussed.

KEYWORDS: Identity management, Digital identity management system, Single Sign-On, Management strategy

Introduction and Related Work

Although the area of digital identity management becomes more and more important in the last few years, only a modest number of related papers can be found in the literature. Software vendors advertising the so called digital identity management systems offer abundance of commercial material and half-technical tips for deployment and configuration, however there is a lack of deeper understanding of directions and good practices. How to make a decision for the right digital identity management system? What to take into account when defining user roles? How to enforce the system use in accordance with existing identity management strategy? Etc.

On the market of identity management systems (IDMS), the main players are, not surprisingly, the well-known software houses: Microsoft, Oracle, IBM, Sun Microsystems, HP,... Besides that, several small or relatively unknown IDMS companies offer allegedly just as good, if not even better products.

Further, let us point out three of the theoretical works. The document [5] is evolving and growing almost for ten years, published several times in different versions and often cited. The author created a detailed taxonomy of terms and ideas in the field of user anonymity, including terms identity, pseudonym and unobservability. In newer document releases, the term identity is broadened and identity management and consequently IDMS-es are introduced.

Clauss et. al. (2001) deal with the concept of multilateral security in communications, which provides security not only for our system users but also for the other party in communication. Not surprisingly, it turns out that the best solution for multilateral security implementation makes use of digital identity management system. Authors also shed light on some common

problems in order to point out a quite lengthy list of requirements for digital identity managers and suggested ways of integration for both systems.

The paper from Hansen et al. (2004) deals with privacy enabling technologies as an answer to legal and social higher and higher privacy expectations and demands. Since technology as a tool is rather unpractical, the authors suggest its use through digital identity management systems. As a consequence, some weak points of today's IDMSes are exposed and an improved concept of IDMS architecture is suggested.

University of Santa Cruz (2007) offers an interesting collection of related documents within its IDMS project web pages. Among them, we would like to point out extensive contents of their general strategy description. Similar, but somewhat narrow is the content of the University of British Columbia (2005) strategic document, which, although a few years old, remains in the draft phase. Nevertheless it sheds light on some digital identity management issues in an innovative way.

The purpose of this paper is as follows. First, it shortly describes the area of digital identity management and some of the most important terms in the area. Further, it describes the basic IDMS building blocks and includes a short discussion of their purpose. In the main part of the paper, a framework of a general IDMS strategy is presented and illustrated with our experiences from a large university environment. We conclude the work with a few comments on our project execution and the lessons learned.

Basic Terms and the Method

To enable deeper understanding of the problem area, first we have to use precisely defined terminology. Therefore we give a set of important definitions in the following subsection (2.1). After that, an agreement has to be made on what do we want to accomplish by introducing a new system, namely IDMS. Therefore, we give the most important goals of identity management in the subsection 2.2. The strategy should be aligned with these goals as much

as possible. The method of building the IDMS strategy at University of Ljubljana *(abbreviated: UL)* is described in subsection 2.3. Throughout the paper, our ideas will be illustrated with fragments of the real strategy case, so we have included the general description of the University system environment directly after the Method section, in subsection 3.1.

Basic terms

As follows from Pfitzmann et. al. (2008), the **identity** of an object is the set of **attributes** that identifies the object within the set of objects. Since the object sets are different, also the attribute sets can be very different and thus the same object can have several (different) identities, related to different circumstances or object sets. The attribute values as well as attribute sets may evolve over time and consequently object identities are not static categories.

Role denotes a set of actions and expected object behavior in given circumstances. Partial object identity or a **pseudonym** is represented by the subset of attributes, corresponding to the object in a given role.

Digital object identity is the set of object attributes, stored, linked and accessible via computer technology.

A broad definition of digital identity management is: planning and control of digital identity data, while digital identity management system (IDMS) represents an infrastructural part with coordinated use of identity management applications and tools. Such a system recognizes different kinds of communication in different conditions and values them against their meaning, functionality, security, privacy and potential risks. By this, system defines, uses and assigns roles to objects.

The users come upon their digital identity at least at login. Although mere checking on username and password is a simple task, IDMSes may be very complex structures and are rarely completely successfully deployed and utilized.

The case: University of Ljubljana information system has more than 70.000 users (the total number of students and employees), distributed over 26 departments (and locations). They access the system on a daily basis and make use of their department's services, central services and also services offered by partner institutions.

Why digital identity management?

Let us take a quick glance at the main goals of digital identity management.

1. Better and more comfortable user service due to a reduced number of identities per user (less separate accounts for different systems). Ultimately, we aim at single sign-on with a single user identity. A single identity also implies a single point for user administration, access control management, and most important, centralized data storage. However such an implementation requires a proper connection to all of the back-end applications and systems as well as a friendly user interface for self-provisioning (if applicable).

2. E-business support: back-end systems may perform user authentication and authorization in a transparent fashion, while users are able to access the data and information services offered by separate systems, even within a single transaction. A set of distributed systems, applications and services may appear as an unique integrated system to its users.

3. Central directory: the user directory is a central point of every IDMS and represents a link towards the identity related data within back-end systems and applications. Properly structured directory reflects an organizational structure and, due to unified

identity management, decreases cost of directory management and synchronization / integration.

4. Organizational structure: proper role assignment creates a snapshot of organizational structure while enabling consistent access rights provisioning and limitation of access on the basis of assigned roles. Users can be treated either individually or within a group – administrators may choose the most convenient way.

5. Workflow management: operational IDMSes enable workflow support even through separate back-end systems or applications. End users involvement is based on their roles. Workflow execution and management environment is not necessarily integrated with the IDMS: the two might be linked in the same way as any other two applications.

6. Provisioning and access control: after a successful logon, the user is able to access the resources, applications, systems and data belonging to his assigned role(s). At the same time, access to other resources is disabled.

7. Security and privacy: user no longer needs to memorize (or, even worse, write down) a number of passwords. Use of group accounts may be discontinued.

Through the rest of the paper we will keep in mind the ideas, present within the above goals. We will include all of the target areas in our strategic framework and illustrate the main issues with our experiences from University of LJUBLJANA identity management strategy and IDMS deployment.

IDMS Strategy Definition: our Method

The first step for our project team was the identity management area research. We have established the terminology (described in 2.1), reviewed the potential benefits of IDMS use (described in 2.2) and tested some of the existing IDMS systems and directory systems. The main sources of information were scientific papers, technical reports and vendor-specific white papers.

The second step was decision on which IDMS functions and benefits do we want to implement, to what extent and what are the priorities? In order to make the right decision, we have had numerous discussions with university management, central IT department members, commission for the information systems development as well as with some local system managers and administrators at faculties or department sites. Since there are almost thirty faculties and departments, we did not consult all the administrators or deans, neither did we perform a special survey. Instead, we made use of documentation and knowledge of the central IT department members. We have confronted the user needs, application requirements, options offered by modern technology as well as the security needs and threats in order to find a rational yet comprehensive solution. After that, we were also required to identify the compatibility requirements, enabling the choice of the central directory and IDMS technology.

The third step embodied the majority of the work, namely the definition of identity lifecycle with the states or phases for different kinds of digital identities in our system. It included answering the related questions (what happens when a new digital identity is created, how does it get new rights, how and when to disable it, and many others). This step represented the core contents of our IDMS strategy. The basic input was the information collected at the previous step, however the whole series of meetings with different stakeholders had to be repeated since now we needed more detailed answers. The output of this step was a document – digital identity management strategy, as described in section 3.

In the next section, we first outline the properties and limitations of our target environment and after that, the main points of identity management strategy are described.

Digital identities in university environment

State of the art and the desired goal

The University of Ljubljana information systems are distributed over its faculties and departments. Only a few applications are common and centralized. Several systems and applications are specific for the department research areas, likely incompatible with other departments' applications and they even make use of own authentication and authorization systems.

With the introduction of Bologna system of study, the mobility of students as well as teaching staff is increased. A mobile person needs access to the university IT infrastructure while on the go and consequently obtains a new digital identity at each new location. This leads to even larger number of digital identities despite the fact that technology enables building of large and complex systems where only one identity per user is a feasible solution.

Long-term goal at University of Ljubljana is a central digital identity management system for students and employees. The system should receive identity-related data from existing databases, especially from the student enrollment and HR databases. The system should offer its services (authentication, identity management...) to the existing applications, while enabling development of new services: unified student e-mail accounts, mailing lists, common calendar, central directory... Digital identity administration will be simplified and some responsibilities will be taken off the local administrators, while security questions will be properly and consistently addressed.

Digital identity management strategy: the framework

The current section represents the core of our work, namely the description of digital identity management strategy. Although not all of the strategic decisions are presented in the following text, none of the important questions are omitted.

All of the employees and students as well as some business and research partners should have a simple, yet safe way to access the university IT resources and services from anywhere over the internet. This need is a major driving force for the open but safe information infrastructure design. At the same time effective and flexible access management processes need to be established together with strict access rules and policies.

Although it is not uncommon that the organization sets the project off when it would already need its results yesterday, the building of identity management system is usually carried on as a series of separate, consecutive IT projects with smaller but clearly defined goals. At University of Ljubljana, such projects might be central directory deployment, unified student e-mail accounts, certificate agency deployment, etc.

Since digital identity management systems are large and complex structures, it is vital that the smaller, partial projects follow the same strategy and respect unified security policies, which maybe even haven't been written yet! The results should guarantee high scalability (tens of thousands users) and high availability (hence redundant infrastructure) together with an appropriately organized IT support and help desk.

Having in mind possible connectivity with other organizations and institutions, the chosen technological solutions should enable standard techniques for identity data federation among disparate identity management systems. At last, security standards should be taken into account (ISO 27001:2005) as well as information process management best practices (ITIL) Thus, a new identity management system will quickly gain confidence from its users.

UL case:

In the process of building its digital identity management system, University of Ljubljana encountered numerous challenges. The expected number of end users is 70 000 and still growing (alumni are not considered yet). The target class of availability is 99.999% - roughly five minutes of down time is allowed per year. A huge investment is needed to provide for the

appropriate system infrastructure and help desk launch. Since a lot of personal data is stored in a system database, we also have to take into account the local legislation on personal data protection and adapt the level of security and access management accordingly. One of the University goals is enabling connectivity with other institutions' directories (Ministry of science and higher education, Slovenian academic and research network...), hence federation is an important technical issue too.

The following subsections survey the most important areas that identity management strategy should cover in any organization. When appropriate, we also give illustrative details, specific for the University of Ljubljana case.

How many identities?

Most organizations tend towards the magical Single Sign-on, namely one digital identity per person. However in larger organizations with colorful background regarding directory technologies and implementations and with heterogeneous applications this goal is hard to achieve. Often the organizations settle for an interim Reduced Sign-On strategy: the number of identities is decreased as much as possible within reasonable limits of organizational effort.

In the phase of strategy design, the organization should decide whether it is possible to make a transition to a single identity in one step or not. If the transition is gradual, the transition phases should be identified and strict rules defined (when new identities may be granted to users, when multiple identities may be kept - for example for the users of a legacy application with specific technology).

UL case:

We were faced with an interesting dilemma when contemplating the role of university employees who are active students at the same time. An identity data in the directory is freely accessible and our legislation does not treat employees in the same way as the

students. All the student data (including student names) should be kept private, while employee data is allowed to be exposed to anybody querying the directory. A student e-mail domain is not the same as employee user domains, etc. These reasons were the basis for our decision to allow two separate identities for such cases, one student identity and one employee identity.

New digital identity

Usually, a new digital identity is created when a new employee comes into an organization. In University environment, there is also a massive creation of new identities each year with a new generation of students. Creation of a new digital identity includes account creation and initial password assignment, while the strategy should include password-related rules: length and complexity, how often the users should change passwords, additional means of identification (i.e. biometric...) etc. When the digital identity is created automatically, strategy should also define activation rules and minimal set of user rights that comes with each identity. Assignment of further roles and privileges as well as provisioning and deprovisioning is up to the system administrators and is done through the digital identity management system.

UL case:

The students get their digital identities within the enrollment process – the user accounts and random passwords are generated automatically. When a student agrees to the terms and conditions of University services use, he is allowed to activate his account, change the initial password and update the data in his user profile. At activation, he is provided with the minimal set of user rights. Since during the course of study the information needs may evolve, the administrators are able to assign new roles and rights, even temporary ones (and withdraw them as well) through the identity management system user interface. When leaving the University, the user account remains active, though it is moved into Alumni

program and most of the roles and rights enabling access to University resources are withdrawn.

The employees get their digital identities as soon as they start working. The digital identity management system monitors data change in HR databases and accordingly creates new identities. Although employee roles differ from student roles considerably, their assignment or withdrawal as well as overall management are similar. Local administrators manage the roles dealing with local infrastructure access, while the global roles regarding overall information services access are managed centrally.

One more thing: by now, we have treated identity somewhat simplistically as a username and password combination. In identity management systems we often use stronger authentication methods or two factor authentication; UL strategy for example requires digital certificates for selected applications and roles.

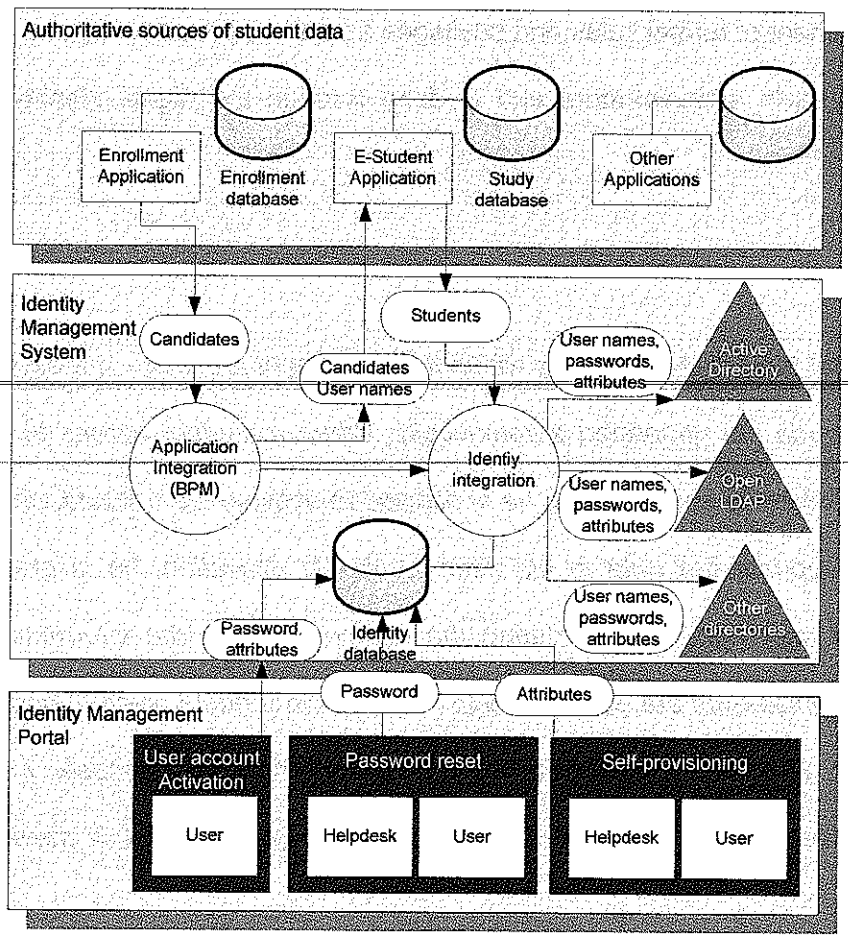


Figure 1: University of Ljubljana System Structure and the process of creation or update of a student identity

A Minimal Set of Rights

When a new digital identity is created, it is assigned a minimal set of rights, as defined by strategy. Strategic decision should precisely define all the rights and privileges, usually at least a new e-mail account in the organization's domain, access e-mail server and intranet and possibly access to common application resources, file servers, collaboration and groupware portals, etc.

UL case:

The strategy defines at least two different minimal sets of rights, one for the students and the other for the employees. The student set contains access to a few applications (e-study application, info points), access to the academic and research wireless network, access to certain library resources, and e-mail account in the University domain. For the employees, a minimal set is somehow smaller: it contains only access to the wireless network, access to certain library resources and an e-mail account. Access to the applications is granted manually on per-user basis.

Assigning new rights and privileges

New roles and access rights are assigned according to the work process and employee roles in the process. Often the system administrators assign roles manually, since only a few kinds of changes can be automated (for example, when employee gets a promotion, his record in HR database is changed. The change may be propagated into the identity management system and his or her roles adjusted automatically).

UL Case:

New roles may be assigned in the following cases: change of work positions, joining a project team, teaching at other departments or locations, etc. Student roles change when joining the

library, enrolling in a new study program or year, finishing the study, joining a project team, etc. Our identity management system allows some automated role changes on the basis of changes in HR and study databases. However the level of automatism is still low because of the back end systems and peculiarities of the legacy applications.

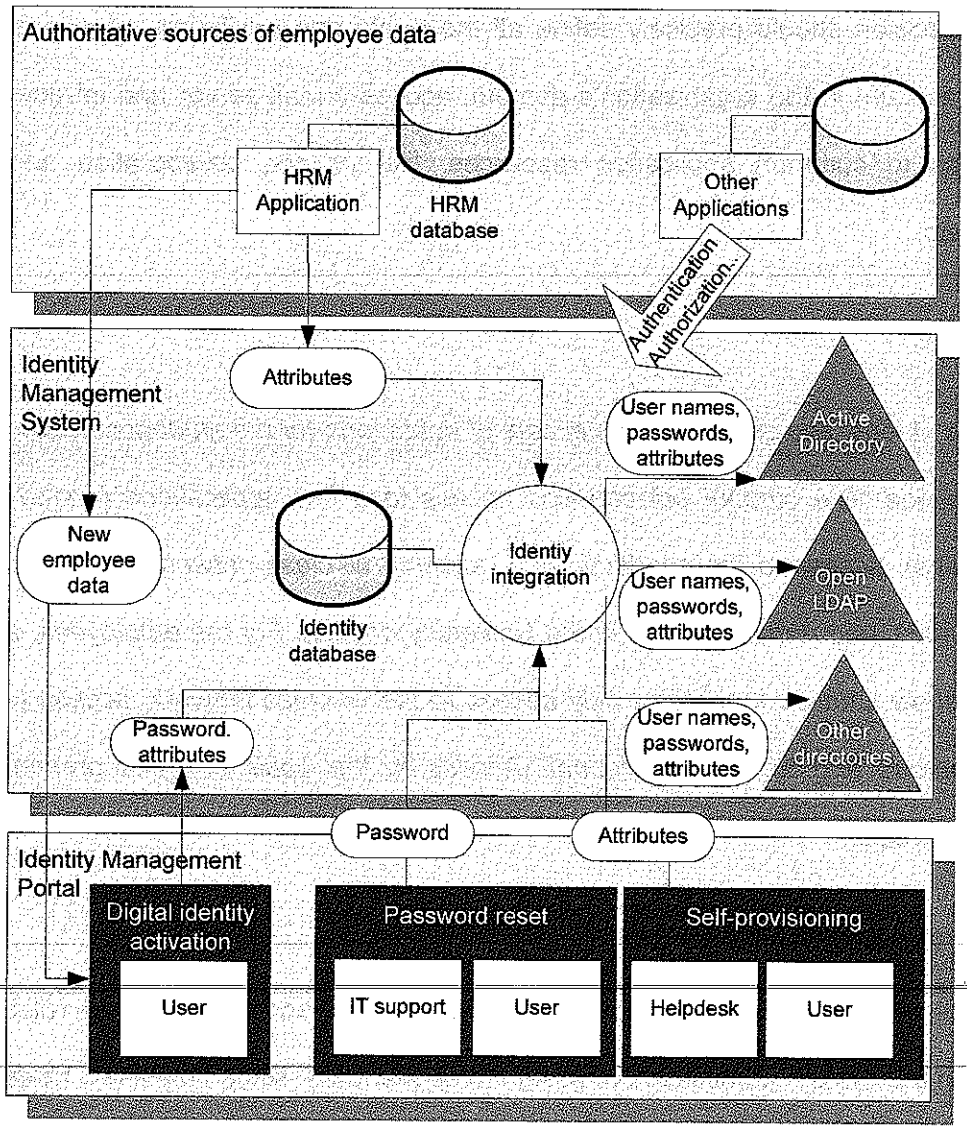


Fig. 2: What happens in the IDMS when a new employee comes?

User groups and security groups

User groups make system administration easier and allow for simpler rights and restrictions assignment consistency. Two approaches to user group creation are possible.

The first approach assumes that equal users are assigned equal roles, thus a user group consists of all the users with the same set of privileges. The second approach presumes that an administrator creates a group object and assigns privileges to the group. After that, he may add users to the group and each user gets all the privileges of the group. In any case, corresponding administrative tools are needed.

UL case:

University system makes no difference among roles and groups. A set of rights, belonging to a certain role, is the same as the set of rights belonging to the corresponding security group in a central directory. Beside global groups, each faculty or department may define its own local groups with arbitrary rights, as long these do not collide with central strategy. The strategy also defines global roles, enabling applications to perform user authentication and authorization. Digital identity management systems can assign these roles automatically, while the administrators are also able to do this manually.

E-mail accounts

Since the content of this section is pretty much straightforward, we will keep it short. An employee should have exactly one e-mail account, just as he or she should preferably have exactly one digital identity. However an e-mail account must never be used as a means of proving his or her identity. This is just one of the attributes within a user profile. On the basis of user roles or other properties email addresses may belong to groups or may belong to distribution lists.

UL case:

UL provides all of the students and employees with e-mail accounts in its domain. Distribution lists are formed for employees on the basis of their working positions and for the students on the basis of their study program, year of study, courses taken etc

Application login and Access to other Services

The preferred way of system access is, as already pointed out, Single Sign-On (SSO). SSO is a goal of the last phase of identity management system launch. For user, SSO means that he or she signs into the web portal, which is integrated with the digital identity management system. From that moment on, the user does not need to sign into other applications because he or she has already been authenticated by the system. If single sign-on isn't feasible due to technical (legacy applications) or organizational issues, direct login into the target application is acceptable as long as the application authenticates users on the basis of the central directory data (campus-wide login principle). This way, every user still needs exactly one username and password although it is used in different places (applications).

Misuse Prevention

Introduction of unified identities and central directory inherently increases the level of security risk accompanying identity theft, since one identity facilitates access to all the information resources. At the system level, we have to use all means to prevent identity misuse, namely make using someone else's identity as hard as possible. In university environment, misuse might be critical when taking exams, and less severe when willingly letting somebody use the identity temporarily to access the system resources. However permanent user education and high level of security awareness are essential. Users need to be aware of the fact that even seemingly harmless identity sharing might end in a serious security violation.

Digital identity management project at the University of Ljubljana

In the previous section, we have described the digital identity framework and also gave some detail, specific for the case of University of Ljubljana. This section moves the focus slightly off the digital identity management strategy and describes the whole project of introducing digital identity management system. Due to the infrastructural heterogeneity, a high number of users and specific organizational issues, building the digital identity management system at University of LJUBLJANA was a great challenge for all the involved personal - technically as

well as organizationally. This is why we believe that not only the strategy framework but also our experiences will be of interest to a wider group of readers.

The project was carried out in several phases, the contents of which can be summarized into the following ten points:

1. Analysis, comparison and a choice of appropriate digital identity management system
2. Digital identity management strategy definition. Digital identity lifecycle definition.
3. Migration strategy to integrated digital identity management system
4. Plan for migration, organization and management of digital identity management system
5. ITIL process definitions for digital identity management
6. Highly available central directory implementation, accessible for other university applications (enrollment, HR...).
7. Pilot launch at one small and one large department or faculty.
8. Testing and debugging.
9. Consequent migration to the remaining faculties.
10. Certificate agency implementation.

Although numbered, the phases needn't be executed exactly in the above order or some of them might be overlapping or executed in parallel. In our case, the last phase is still to be accomplished.

The solution architecture has three key parts: central directory, identity synchronization system and digital certificate management system. In the early phases, one of the most important activities was development of a system plan, including system properties such as high availability, high performance, robustness, technology and software demands, naming standards etc. The plan guarantees correct data synchronization and continuous data availability as well as the desired performance level, according to the existing network topology and other infrastructure technology.

Another key activity was the development of a transition strategy for integrated digital identity management system, including unified identity protection. The transition strategy consists of six key areas:

a) Central directory naming standards,
b) Employee identities migration from existing directories to the new central directory.
c) Lifecycle and management of student identities
d) Lifecycle and management of employee identities
e) Mapping and updating attributes between central directory and back end systems.
f) Suggestions regarding new applications integration: rules on how to authenticate user, which attributes to use etc.

In the time of writing this paper, a central directory is implemented and its database size is estimated on 15 GB. The first new application, using all the benefits of IDMS, is beginning its production phase.

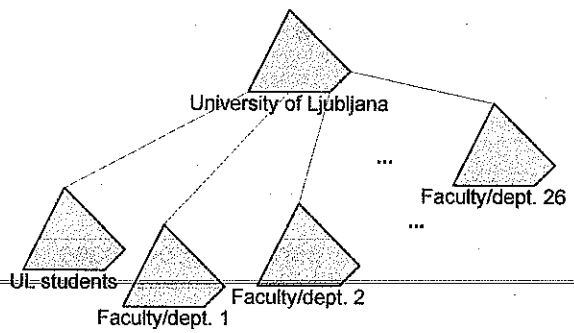


Fig 3: Directory structure – university forest.

Before we could start the systems synchronization processes, the directory and domain name servers had to be configured. Further, the rules on when, what and how to synchronize were implemented. The purpose of the synchronization is a controlled flow of digital identity data between the central database and backup systems.

The third IDMS system component is the whole architecture of university certificate agency - digital certificate issuing servers. Use of digital certificates enables advanced security scenarios in the university network; a few examples are secure network logon, smart card user identification, server identification and authentication, etc. Our solution employs two-level certificate authority: at the top level there is an independent, off-line root certification authority - a server that issues certificates to the second level, networked certificate issuing servers. These issue certificates to other university servers as well as to users. Both kinds of certificate issuing servers have to be highly secured and protected.

The deployment plan should ensure appropriate system response times and enough redundancy to achieve high system fault tolerance. Sufficient processing power and proper network capacities contribute to short response times, while fault tolerance is achieved by the server replication: in root domain, there are three domain controllers and two DNS servers, while the domain controllers in the subdomains are duplicated. Minimal hardware requirements for servers are calculated with regard to the domain size and the estimated number of users. Virtualization is only allowed to the certain extent, enabling efficient hardware utilization while not impairing fault tolerance.

Among the lessons learned, there are a few obvious ones: plan in advance, learn from experiences of others, include the main players already in the early phases. However, an interesting negative experience was that we have followed an advice on system architecture from one of the main players on the digital identity market. At the end, the architecture proved to be far too complicated, synchronization processes lengthy and the servers underutilized. This is the issue that we would have definitely deal better with on our own. Stick with a simple architecture!

On the other hand, an important lesson was also not to include too many players. When a project team becomes too big, it is virtually impossible to reach an agreement. So rightsizing is the keyword, together with a proper judgement about who is a main player and who is not.

Regarding the strategy contents, be prepared to compromise. For example: certainly one would want to have a secure information system and authenticate users with digital certificates. But from usability point of view, we have decided that the students are not required to use certificates (although they may opt so), because many of them would want to use the system from a cyber café or from a friend's computer, where smart card reader may not be available.

Conclusions

Since identity management is becoming an important part in the systems management area, in our paper we made an overview of all the key points. However we could not cover the whole process of building and deploying a new IDMS. For example, we left out the series of questions like "What happens in the IDMS database when the data is changed at the authoritative source?" and other questions, dealing with data consistency. There will always be a lot of questions that each project group will have to face in their own way.

However we did sketch the process of IDMS building and we described the IDMS strategy framework and its basic contents, which is the crucial part of successful IDMS deployment. University of LJUBLJANA faced all the described problems and dilemmas and despite several unexpected technical and organizational obstacles, the project is entering its closing phase. Especially because of this practical experience that lies behind the paper, we hope and believe that the described experience will be interesting as well as informative reading for everyone taking part in or contemplating on a similar IDMS project.

Bibliography:

1) UC Santa Cruz (2007): Identity Management Project Documents, accessible at http://its.ucsc.edu/idm/doc_index.php (July 2007).

2) University of British Columbia (2005): Identity Management Strategy draft v1.03, February 2005, accessible at http://www.e-strategy.ubc.ca/_shared/assests/IDMS-strategy-11932.pdf (July 2008).

3) HANSEN M, BERLICH P, CAMENISCH J et.al. (2004) Privacy-enhancing identity management, Information Security Technical Report, Volume 9, Issue 1, Elsevier Ltd., January-March 2004, pp. 35-44, doi:10.1016/S1363-4127(04)00014-7.

4) CLAUSS S, KOEHNTOPP M (2001). Identity Management and Its Support of Multilateral Security, Computer Networks, vol. 37 (2001), *Special Issue on Electronic Business Systems*, Elsevier, North-Holland, pp. 205–219.

5) PFITZMANN A, HANSEN M (2008): Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v0.31 Feb. 15, 2008). Accessible at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

6) AUTHORS (2008): Strategy of Digital Identity Management at the University of LJUBLJANA, Technical report v1.0, University of LJUBLJANA, April 2008.