UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Marko Kuhar

Sistemi za upravljanje z digitalnimi identitetami

DIPLOMSKO DELO

NA UNIVERZITETNEM ŠTUDIJU

Mentor:

doc. dr. Mojca Ciglarič

Ljubljana, 2010

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01600/2009
Datum: 15.10.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MARKO KUHAR**

Naslov: **SISTEMI ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI**
DIGITAL IDENTITY MANAGEMENT SYSTEMS

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Preglejte in analizirajte področje upravljanja z digitalnimi identitetami. Definirajte najpomembnejše pojme. Navedite in opišite komponente sistemov za upravljanje z digitalnimi identitetami in njihove medsebojne odnose in odvisnosti. Opišite in razložite zivljenjski cikel uporabnika in oskrbovanje uporabnikov ter arhitekturo za njegovo podporo. V praktičnem delu preglejte obstoječe izdelke na trgu ter izberite dva, ki se po izbranih kriterijih zdita najbolj zanimiva. Preizkusite ju v tipičnih situacijah ter kritično ovrednotite prednosti in slabosti.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:
prof. dr. Franc Solina

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01600/2009
Datum: 15.10.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MARKO KUHAR**

Naslov: **SISTEMI ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI**
DIGITAL IDENTITY MANAGEMENT SYSTEMS

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Preglejte in analizirajte področje upravljanja z digitalnimi identitetami. Definirajte najpomembnejše pojme. Navedite in opišite komponente sistemov za upravljanje z digitalnimi identitetami in njihove medsebojne odnose in odvisnosti. Opišite in razložite zivljenjski cikel uporabnika in oskrbovanje uporabnikov ter arhitekturo za njegovo podporo. V praktičnem delu preglejte obstoječe izdelke na trgu ter izberite dva, ki se po izbranih kriterijih zdita najbolj zanimiva. Preizkusite ju v tipičnih situacijah ter kritično ovrednotite prednosti in slabosti.

Mentor:

doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:

prof. dr. Franc Solina

ZAHVALA

Rad bi izrazil hvaležnost vsem, ki so kakorkoli pripomogli k uspešni izvedbi tega diplomskega dela.

Zahvaljujem se mentorici, doc. dr. Mojci Ciglarič za usmeritev pri izbiri teme, nasvete in vodenje pri izdelavi diplomskega dela.

Diplomo posvečam svoji družini, ki me je vsa ta leta podpirala in mi omogočila študij. Hvala.

Posebna zahvala gre moji Maji - za moralno podporo, potrpežljivost in večni optimizem.

KAZALO VSEBINE

SEZNAM UPORABLJENIH KRATIC

ACL	*ang. Access Control List* - Seznam za kontrolo dostopa.
CD	*ang. Connected Directory* - Oddaljen podatkovni izvor.
CLM	*ang. Microsoft Certificate Lifecycle Manager*
CS	*ang. Connector Space* - Področje ILM repozitorija, ki se uporablja za shranjevanje kopij podatkov iz različnih CD-jev, na katere smo povezani.
DIT	*ang. Directory Information Tree*
DNS	*ang. Domain Name System* - Sistem domenskih imen.
ERM	*ang. Enterprise Role Management* - *S*istemi za obvladovanje poslovnih pravil.
IAM	*ang. Identity and Access Management* - Upravljanje identitet in dostopov.
IDA	*ang. Identity Audit* - Revizija upravljanja identitet.
IDM	*ang. Identity management* - Upravljanje z digitalnimi identitetami.
IDMS / IMS	*ang. Identity Management System* - Sistemi za upravljanje z digitalnimi identitetami.
ILM	*ang. Identity Lifecycle Manager* - Blagovna znamka podjetja Microsoft za linijo izdelkov, ki spadajo v segment upravljanja identitet in dostopov.
ITU-T	*ang. International Telecommunication Union - Telecommunication Standardization Sector*
LDAP	*ang. Lightweight Directory Access Protocol* - Preprost protokol za dostop do imenika.
LDIF	*ang. LDAP Data InterChange Format* - Tekstovni format za opis informacij iz imenika LDAP.
MA	*ang. Management Agent* - Je komponenta ILM, ki poveže oddaljen podatkovni izvor z ILM in izvede operacije izvoza in uvoza.
MIIS	*ang. Microsoft Identity Integration Server 2003* - Predhodnik ILM.
MMS	*ang. Microsoft Metadirectory Services* - Predhodnik MIIS.
MV	*ang. Metaverse* - ILM meta imenik.
OIM	*ang. Oracle Identity Manager* - Blagovna znamka podjetja Oracle za sistem, ki spada v segment upravljanja identitet in dostopov.
PKI	*ang. Public Key Infrastructure* - Infrastruktura javnih ključev.
SOD	*ang. Separation of duties* - Politika razčlenjevanja vlog.
SPML	*ang. Service Provisioning Markup Language* - Označevalni jezik za storitve oskrbovanja uporabnikov.
SSO	*ang. Single Sign-On* - Enotna prijava.

POVZETEK

Cilj diplomskega dela je pregled obstoječih sistemov in tehnologij za upravljanje z digitalnimi identitetami ter izbira in nato podrobna primerjava dveh najbolj obetavnih sistemov za neko tipično okolje.

V prvem sklopu diplomskega dela sem najprej predstavil teoretične osnove, ki so pomembne pri razumevanje tematike upravljanja z digitalnimi identitetami. Pojasnil sem razliko med identiteto in digitalno identiteto ter odgovoril na vprašanje kaj je to upravljanje z digitalnimi identitetami. Na posplošenem primeru sistema za upravljanje identitet sem razložil vse relevantne pojme, komponente in tehnologije, ki sestavljajo to področje. Posebno pozornost sem namenil segmentu oskrbovanja uporabnikov, kjer sem na generičnem arhitekturnem modelu predstavil gradnike teh sistemov.

V drugem sklopu diplomskega dela sem s primeri osvetlil lastnosti IDM sistemov, ki zmanjšujejo stroške za informatiko, nadalje prednosti, ki jih občutijo končni uporabniki in kako se zaradi vpeljave le-teh izboljša varnost na ravni celotne organizacije. Izpostavil sem razliko med celovitimi in delnimi sistemi za upravljanje identitet. V nadaljevanju sem identificiral vodilne proizvajalce celovitih sistemov, kakor tudi sistemov za oskrbovanje uporabnikov ter slednje na kratko predstavil.

Tretji sklop diplomskega dela se začne z opisom evolucije, lastnosti, arhitekture ter podprtih okolij sistemov Oracle Identity Manager in Microsoft Identity Lifecycle Manager. V nadaljevanju sem definiral problemsko domeno, ki predstavlja tipičen administratorski problem iz realnega sveta. Nato sem na podlagi implementacije scenarija problemske domene, primerjal zgoraj omenjena sistema za oskrbovanje uporabnikov. Na ta način sem spoznal in tudi v praksi uporabil oba sistema. Opisal sem potrebne korake za realizacijo scenarija, pojasnil konfiguracijo in izpostavil izkušnje, ki sem jih pridobil pri tem. Tako sem se dokopal do spoznanja, da Oraclov sistem potrjuje svoj status vodilnega sistema na področju oskrbovanja uporabnikov.

Ključne besede:

- Upravljanje z digitalnimi identitetami,
- Oskrbovanje uporabnikov,
- Oracle Identity Manager,
- Microsoft Identity Lifecycle Manager

ABSTRACT

The goal of this thesis is a review of existing systems and technologies for managing digital identities. After the selection of the two most promising systems there will be a detailed comparison for a typical environment.

In the first part of my thesis, the theory for understanding issues of identity management is introduced. Furthermore, the difference between identity and digital identity is explained and identity management itself is interpreted. An example of identity management solution outlines all the relevant concepts, components and technologies that make up this area. Special attention was made on the user provisioning segment, where a generic architecture model presents all the components of these systems.

In the second part of the thesis, I highlight examples of aspects in IDM systems that reduce costs for IT, further benefits to end-users and how the result of applying them improves safety at the entire organization level. I discuss the difference between Identity and Access Management Suites and Point Identity and Access Management products. In the second part, I have identified leading vendors of Identity Management Suites, as well as User provisioning systems, the latter with a brief presentation.

The third part of the thesis begins with a description of the evolution, characteristics, architecture and environments supported by the systems Oracle Identity Manager and Microsoft Identity Lifecycle Manager. Here I define a problem domain, which is a typical real world administrator problem. Then, based on the implementation scenario of the problem domain, the above-mentioned systems for User provisioning are compared. In this, way I gained practical experience in both systems. I described the necessary steps for the realization of my scenario, explain the configuration and highlighted the experience I have gained in doing so. Finally I came to the conclusion, that Oracle is confirming its status as the leading vendor in the User provisioning field.

Keywords:

- Identity management,
- User provisioning,
- Oracle Identity Manager,
- Microsoft Identity Lifecycle Manager

Poglavje 1:

UVOD

1.1. Uvod v tematiko

Z razvojem kompleksnosti poslovanja organizacij in večanjem števila zaposlenih se je povečevalo tudi število programskih aplikacij, ki jih le-te uporabljajo pri obvladovanju vsakodnevnega dela. Vse večja informatizacija poslovanja je pripeljala do tega, da tudi dobavitelji ter ostali partnerji potrebujejo dostop do virov znotraj organizacije. V ne tako davni preteklosti sploh ni bilo strogih dostopnih politik in zaposleni, ki so imeli dostop do računalnika, so lahko brez omejitev dostopali do vseh virov znotraj organizacije. Združbe so se le sčasoma začele zavedati, da morajo zaščititi dostop do svojih informacijskih virov in sredstev. To je privedlo do razmaha aplikacij, ki so uporabljale sebi lastne avtentikacijske mehanizme in zaposleni so potrebovali uporabniško ime in geslo, ki sta predstavljala identiteto, prav za vsako posamezno aplikacijo. Zaradi zapletenosti tematike je bil poslovni management nemočen pri preverjanju varstva zasebnih podatkov in nadziranju zaposlenih pri dostopanju do občutljivih informacijskih virov znotraj organizacije.

Večina organizacij ima težave z upravljanjem in nadzorom vseh svojih uporabniških identitet in gesel še danes, ker so raztreseni med različnimi informacijskimi sistemi. S hitrim razvojem informacijske ter omrežne tehnologije pa postaja problem za vse združbe po svetu (vlade, podjetja, univerze) še bolj pereč. Dodatno ga zapleta mobilnost ljudi. Organizacija je dinamična tvorba, nekateri jo zapuščajo, drugi v njo vstopajo, spet tretji napredujejo in se jim zaradi tega spremeni vloga. Zato je zelo težko jamčiti, da ima vsak uporabnik dostop do ustreznih informacijskih virov, ki so skladni z njegovo vlogo. [**15**,**30**].

Sistemi za upravljanje z digitalnimi identitetami rešujejo zgoraj opisane težave.

1.2. Namen in cilji

Diplomsko delo sem razdelil na tri sklope. V prvem, teoretično-tehnološkem sklopu diplomskega dela želim:

- Opredeliti osnovne pojme ter definicije za razumevanje tematike upravljanja identitet.
- Odgovoriti na vprašanje kaj je to upravljanje z digitalnimi identitetami.
- Prikazati osnovne funkcije in zgradbo na posplošenem primeru sistema za upravljanje identitet.
- Predstaviti komponente in tehnologije, ki sestavljajo področje upravljanja z digitalnimi identitetami oziroma le-ta sloni na njih in jih nekako umestiti v celotno ogrodje.

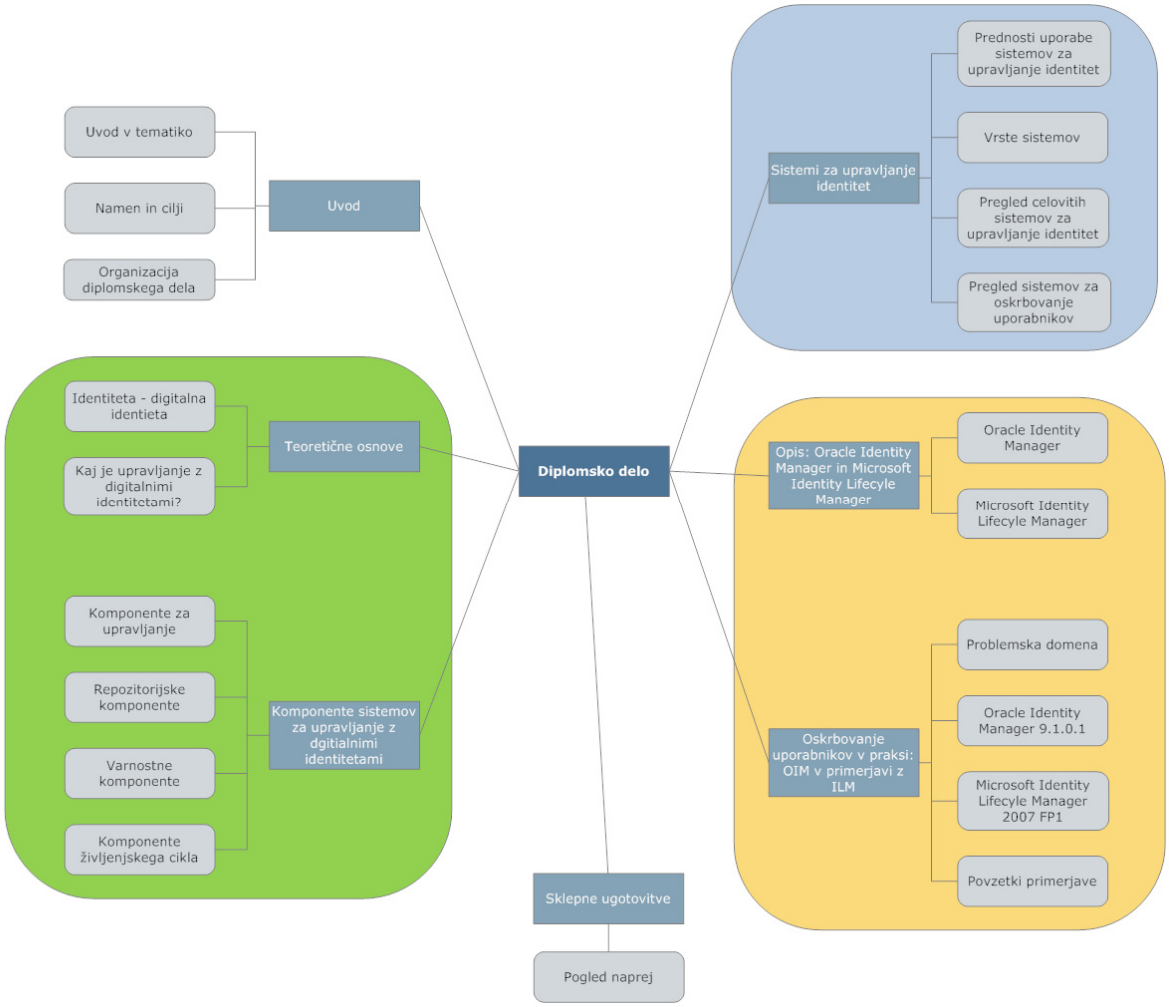
V drugem sklopu diplomskega dela se lotevam tematike iz poslovnega vidika. Glavni poudarki bodo:

- Osvetliti poslovne koristi za organizacijo, ki jih prinese uporaba sistemov za upravljanje z digitalnimi identitetami v praksi.
- Izpostaviti razliko med obema vrstama sistemov za upravljanje identitet.
- Identificirati vodilne proizvajalce celovitih sistemov za upravljanje identitet in vodilne proizvajalce sistemov za oskrbovanje uporabnikov.
- Pregled in kratka predstavitev trenutno vodilnih ponudnikov na trgu sistemov za oskrbovanje uporabnikov.

Tretji sklop diplomskega dela se bo vrtel okoli mojih izkušenj, pridobljenih na podlagi praktične primerjave dveh sistemov za oskrbovanje uporabnikov:

- Primerjavo bom izvedel na podlagi problemske domene, ki bo predstavljala nek tipičen administratorski problem iz realnega sveta.
- Sistema bom izbral na osnovi pregleda trga sistemov za oskrbovanje uporabnikov.
- Izbral bom enega izmed vodilnih ponudnikov ter enega izmed izzivalcev.
- Opisal bom njune lastnosti, arhitekturo, namestitev in konfiguracijo sistemov, potrebnih za pravilno delovanje.
- Z implementacijo scenarija problemske domene bom v praksi testiral kompleksnost in funkcionalnost obeh izbranih sistemov za oskrbovanje uporabnikov.

1.3. Organizacija diplomskega dela



Slika 1.1: Organizacija diplomskega dela

V diplomskem delu so obravnavane naslednje teme:

- *Poglavje 1:* **»Uvod«**
- *Poglavje 2:* **»Teoretične osnove«**
- *Poglavje 3:* **»Komponente sistemov za upravljanje z digitalnimi identitetami«**
- *Poglavje 4:* **»Sistemi za upravljanje identitet«**
- *Poglavje 5:* **»Opis: Oracle Identity Manager in Microsoft Identity Lifecycle Manager«**
- *Poglavje 6:* **»Oskrbovanje uporabnikov v praksi: OIM v primerjavi z ILM«**
- *Poglavje 7:* **»Sklepne ugotovitve«**

Poglavje 2:

TEORETIČNE OSNOVE

2.1. Identiteta - digitalna identiteta

Že sam izraz »upravljanje z digitalnimi identitetami« nakazuje, da pojem »identiteta« igra pomembno vlogo v pričujočem delu. Za popolno razumevanje ciljev upravljanja z digitalnimi identitetami, moramo najprej razumeti pojem identitete.

Identiteta je zapleten pojem z mnogimi odtenki, od filozofskih do praktičnih. Slovar slovenskega knjižnega jezika definira pojem identiteta kot skladnost, ujemanje podatkov z resničnimi dejstvi, oziroma znaki. Kadar je govora o identiteti posameznika, imamo v mislih niz znanih informacij o tej osebi. V računalništvu je identiteta posameznika običajno imenovana digitalna identiteta. Posameznik ima lahko več digitalnih identitet.

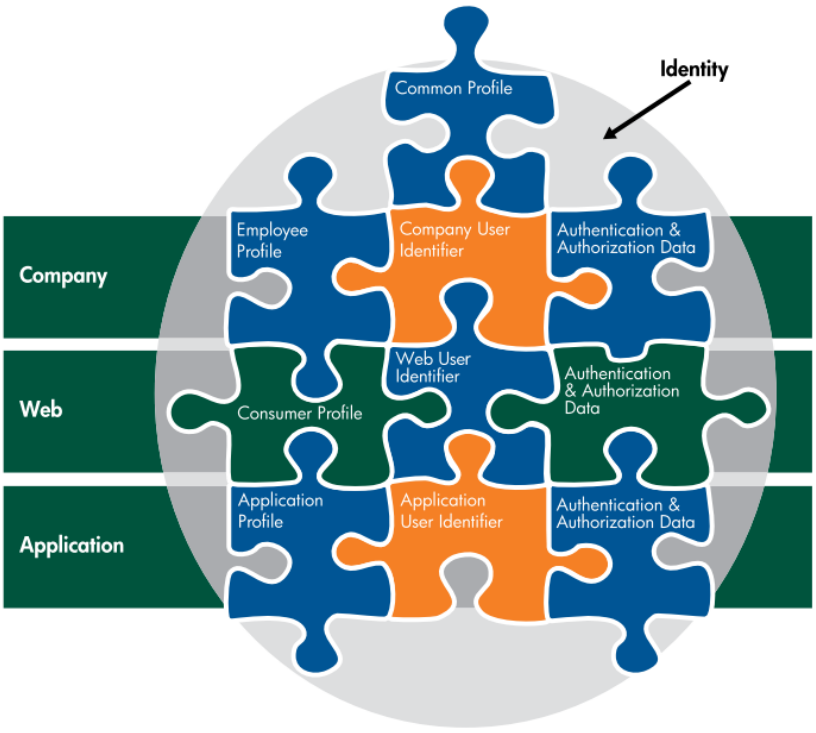
Čeprav digitalne identitete pretežno povezujemo z ljudmi, pa to ni pravilo. Digitalne identitete se vedno bolj nanašajo tudi na nečloveške entitete, kot so storitve, sistemi in naprave, ki se bodo v prihodnosti uporabljale za delovanje v imenu ljudi. [**12**]

Identiteta je edinstven niz podatkov (znak, ime, prstni odtis, številka socialnega zavarovanja, itn.), združen z atributi, ki enolično opisujejo entiteto. Entiteta je lahko uporabnik, aplikacija ali storitev. Identitete so najprej preslikane oziroma v povezavi z določenimi posamezniki ali storitvami, šele nato se z njimi upravlja v okviru konteksta sistemov za upravljanje identitet. Identiteta enolično določa kdo in kaj lahko dostopa do informacijskega sistema. Poenostavljen pogled na identiteto je objekt, kot je recimo uporabniško ime, ki je popolnoma unikatno v določenem sistemu. Ta edinstven objekt

ima vedno vsaj enega ali več atributov oziroma pridevnikov, ki ga opisujejo. Brez atributov tudi identiteta ne obstaja.[**6**]

Vsebina identitete je ključnega pomena pri upravljanju digitalnih identitet *(ang. Identity management, krat. IDM)*. IDM sistem je sposoben upravljati z digitalnimi identitetami glede na njihovo vsebino. Ta se običajno razlikuje glede na kontekst, v katerem se uporablja in vlogo, ki jo ima posameznik v tem kontekstu.

»Slika 2.1« prikazuje vsebino identitete v treh različnih kontekstih: v podjetju, v spletni trgovini ter kot uporabnik aplikacije. Sestavljena je iz enoličnih identifikatorjev posameznika, avtentikacijskih in avtorizacijskih podatkov ter podatkov uporabniškega profila. Vsakega izmed naštetih identifikatorjev je mogoče povezati v različnih kontekstih (podjetje, splet, aplikacija) in vlogo, ki jo ima posameznik v tem kontekstu (zaposleni, stranka, uporabnik aplikacije).



Slika 2.1: Vsebina identitete v treh različnih kontekstih [11]

V realnem svetu je identiteta posameznika lahko sestavljena iz niza imen, naslovov, vozniškega dovoljenja, potnega lista, področja zaposlitve, itn. Ti podatki se lahko uporabljajo za identifikacijo, avtentikacijo in avtorizacijo:

- *Ime* se lahko uporabi kot identifikator - to nam omogoča, da se sklicujemo na posamezno identiteto ne, da bi naštevali vse njene atribute.

- *Potni list* bi lahko uporabili za avtentikacijo - potni listi so izdani s strani ustreznih overiteljev, kar nam omogoča preverjanje pristnosti posameznika.
- *Vozniško dovoljenje* nam podeljuje pravico za opravljanje motornega vozila.

Enolični identifikatorji se lahko uporabljajo v različnih kontekstih. V zgornjem primeru je lahko npr. vozniško dovoljenje enolični identifikator za interakcijo s prometno policijo. Kombinacija imena, priimka ter naslova pa enolični identifikator za pošto in vse ostale dostavne storitve.[**12**]

Iz primerov je razvidno, da vsebina identitete zagotavlja informacije za tri ključne vidike IDM sistemov: identifikacijo, avtentikacijo in avtorizacijo. Te tri komponente so tudi sestavni deli nadzora dostopa v IDM sistemih. S tem, da je identifikacija vključena v komponento za preverjanje pristnosti (avtentikacijo). Več o tem bo razloženo v »poglavju 3.3. Varnostne komponente«.

2.2. Kaj je upravljanje z digitalnimi identitetami?

Bistvo upravljanja z digitalnimi identitetami je zagotavljanje kombinacije procesov in tehnologij, ki nudijo upravljanje in varen dostop do informacij ter virov organizacije, ob hkratni zaščiti uporabniških profilov. Upravljanje identitet ponuja zmogljivosti za učinkovito upravljanje teh procesov, tako za notranjo in zunanjo organizacijo, kakor tudi za zaposlene, stranke, partnerje in aplikacije. Skratka za vse, ki potrebuje interakcijo z organizacijo.[**24**].

Zaradi povečanega interesa pri upravljanju digitalnih identitet v zadnjih petih do desetih letih, številni analitiki in komentatorji ponujajo svoje poglede in s tem povezane definicije za pojem »upravljanja identitet«. Spodaj podajam izbor nekaterih definicij:

Hurwitz Group, 2001:

Poudarek pri upravljanju identitet je na oskrbovanju uporabnikov - ustvarjanju, vzdrževanju in izbrisu uporabniških računov in upravljanju poverilnic za podporo avtentikaciji in nadzoru dostopa.[**24**]

IDC, 2008:

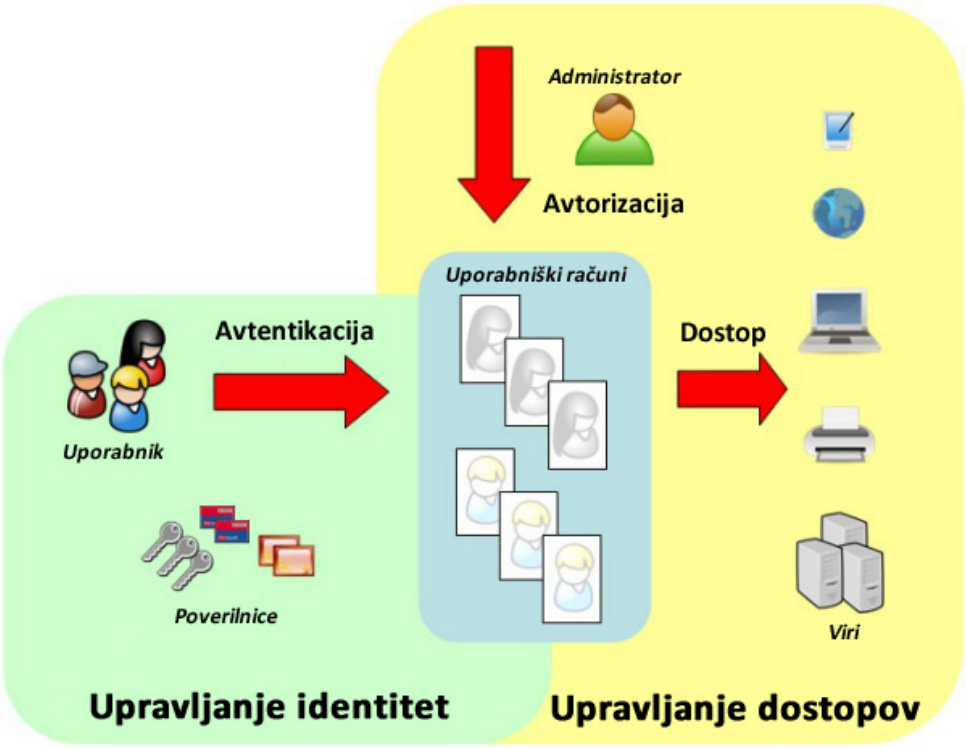
Upravljanje identitet in dostopov je celovit nabor rešitev, ki se uporabljajo za identifikacijo uporabnikov v sistemu (zaposleni, kupci, izvajalci, itd.) ter nadzor dostopa do virov znotraj tega sistema. Na posameznikovo identiteto so vezane uporabniške pravice in omejitve.[**14**]

Wikipedia, 2009:

Upravljanje identitet je integriran sistem poslovnega procesa, varnostnih smernic in tehnologij, ki omogoča organizacijam lažji nadzor uporabniških dostopov do kritičnih spletnih aplikacij ter

informacijskih virov - ob hkratnem varovanju zaupnih osebnih in poslovnih podatkov pred nepooblaščenimi dostopi.[**34**]

V strokovni literaturi se pogosto uporablja kot sinonim terminu »upravljanje identitet« (IDM), tudi termin »upravljanje identitet in dostopov« (*ang. Identity and Access Management, krat. IAM).* Izbira enega ali drugega izraza je odvisna od proizvajalca in kontekst v katerem se uporablja. Izraz »IAM« je morda bolj opisni, saj poleg upravljanja življenjskega cikla identitet uporabnikov, vključuje tudi zunanji nadzor dostopa. Nekateri proizvajalci uporabljajo še variacijo obeh sopomenk »IDA« oziroma »Identity Access« *(slov. dostopi identitet)*. V vseh treh terminih gre za isti pomen.



Slika 2.2: Upravljanje digitalnih identitet in dostopov

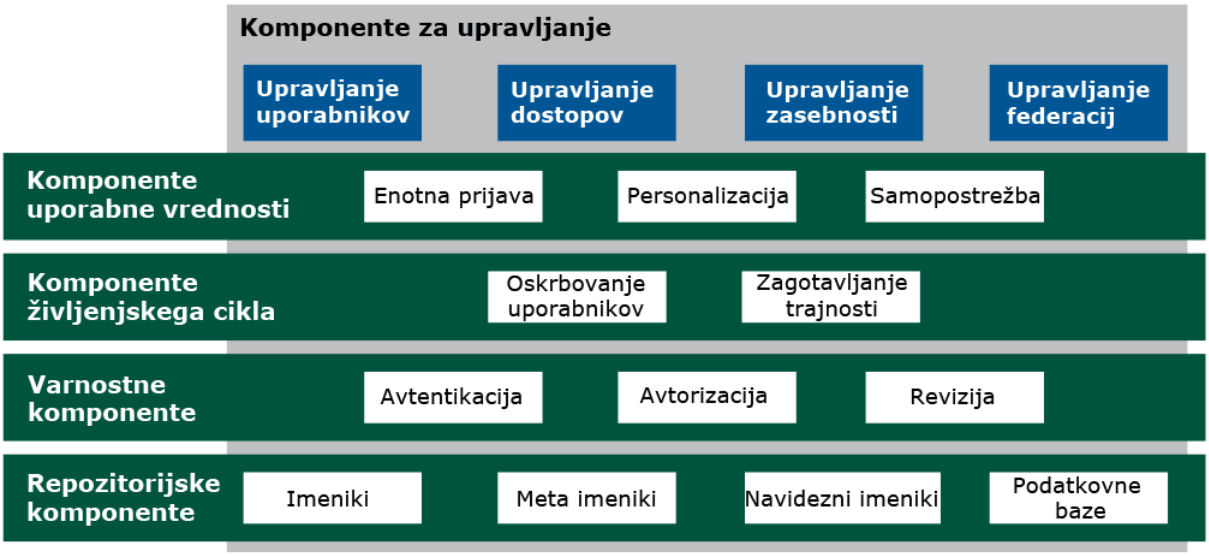
- Pojem upravljanja identitet vključuje upravljanje uporabnikov, katerih digitalna identiteta je shranjena v enem ali več uporabniških računih oziroma profilih. Pripadnost uporabnika določenemu računu se preverja s pomočjo avtentikacije oziroma overjanja.
- Upravljanje dostopov *(ang. Access management)* je postopek, ki
  - določa niz dovoljenj in privilegijev, na podlagi katerih lahko uporabniški račun upravlja z viri, ki so na voljo
  - podeljuje in nadzoruje pravice, katere omogočajo ali preprečujejo dostop do virov[**6**]

Ostale podrobnosti različnih konceptov in definicij bodo obravnavane v naslednjih poglavjih tega dela.

Poglavje 3:

KOMPONENTE SISTEMOV ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI

V preteklosti so bila razvita številna administrativna orodja in sistemi, ki so podpirala upravljanje identitet, neodvisno drug od drugega in na različne načine. Zato se izvirni sistemi za upravljanje identitet funkcionalno zelo prekrivajo. Organizacija teh sistemov v neko popolno ogrodje oziroma arhitekturo za upravljanje identitet je zato zelo težavno opravilo. Sistemi za upravljanje identitet so modularni in sestavljeni iz več storitev in sistemskih komponent.

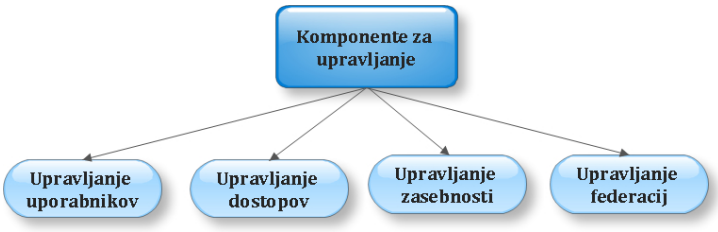


Slika 3.1: Komponente in tehnologije sistemov za upravljanje z digitalnimi identitetami [11]

Ogrodje, kot ga prikazuje »Slika 3.1« je v bistvu posplošen primer sistema za upravljanje identitet. To ogrodje, ki temelji na analizi, povzeti iz virov [**11**,**12**] bom v pričujočem poglavju razširil z dodatnimi informacijami ter opisi posameznih komponent in tehnologij, ki ga sestavljajo.

3.1. Komponente za upravljanje

Pod komponente za upravljanje *(ang. Management Components)* spadajo naslednja področja upravljanja z digitalnimi identitetami: upravljanje uporabnikov *(ang. User management),* upravljanje dostopov *(ang. Access control management),* upravljanje zasebnosti *(ang. Privacy management)* in upravljanje federacij *(ang. Federation management).*



Slika 3.2: Komponente za upravljanje

Zgoraj naštete komponente pokrivajo in opisujejo vsa področja delovanja IDM sistemov. Sledi kratka predstavitev komponent za upravljanje, ki bo dala jasnejšo predstavo o obstoječih tehnologijah, obravnavanih v nadaljevanju tega poglavja.

3.1.1. Upravljanje uporabnikov

Upravljanje uporabnikov nudi administratorjem osrednjo infrastrukturo pri upravljanje uporabniških profilov in prednostnih informacij povezanih z njimi. Poleg tega omogoča organizacijam zmanjševanje izdatkov, namenjenih za informatiko, saj uporabnikom zagotavlja samopostrežne funkcije za preproste administratorske operacije (glej »poglavje 3.5.3«). Z možnostjo optimizacije obstoječih imenikov ter sinhronizacijo uporabniških profilov pa se poveča tudi vrednost obstoječih naložb v informatiki.[**12**]

3.1.2. Upravljanje dostopov

Upravljanje dostopov nudi administratorjem osrednjo infrastrukturo za upravljanje uporabniških avtentikacij in avtorizacij. Z avtomatizacijo varnostnih politik in s storitvami za upravljanje in nadzor dostopa se za zaposlene, stranke ter partnerje povečuje varnost. Hkrati s tem se zmanjšuje zapletenost in skupni stroški namenjeni za informatiko.[**12**] Upravljanje dostopov sestoji iz treh

ključnih komponent: identifikacije, avtentikacije in avtorizacije, ki so razložene v »poglavju 3.3« tega dela.

3.1.3. Upravljanje zasebnosti

IDM sistemi zagotavljajo zasebnost uporabnikov in upoštevajo politike varovanja podatkov, ki so lahko določene s strani organizacije, zakonodajalca ali standardov v industriji.[**12**]

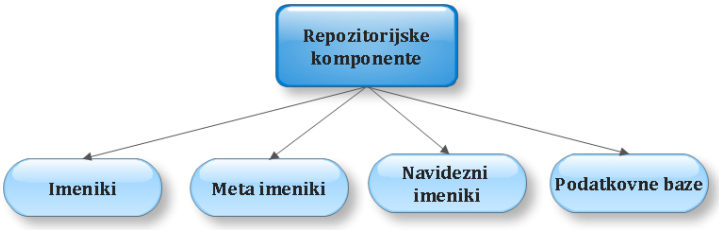
3.1.4. Upravljanje federacij

Federacija je modul ali samostojna komponenta sistemov za upravljanje z digitalnimi identitetami *(ang. Identity Management Systems, krat. IDMS/IMS)*, ki vzpostavlja »omrežje zaupanja«. Federacija pomeni delitev identitet uporabnikov s tretjimi pogodbenimi strankami z namenom združevanja storitev. Ta metoda je zelo uporabna pri poslovnih partnerjih, ki se medsebojno dogovorijo kako in na kakšen način bodo overjali in avtorizirali uporabnike, ki jim bodo zaupali. Uporabnik, ki ga overi eden izmed IDM sistemov v federaciji lahko transparentno preide v poslovno okolje drugega poslovnega partnerja, ne da bi se pri tem moral ponovno avtenticirati.[**5**]

Federacija torej rešuje težave pri upravljanju identitet zunanjih uporabnikov. Federacijske storitve omogočajo varno izmenjavo podatkov z zunanjimi sistemi in s tem razširitev IDM infrastrukture tudi na pogodbene stranke.[**28**]

3.2. Repozitorijske komponente

Velik izziv pri upravljanju digitalnih identitet še vedno ostaja, kako združiti in sinhronizirati uporabniške podatke razpršene med različnimi imeniki v heterogenem okolju. Repozitorijske komponente *(ang. Data repository components)* IDM sistemov delujejo, kot centralna skladišča za uporabniške podatke, ki jih pridobijo iz različnih poslovnih aplikacij ter ostalih imenikov in relacijskih podatkovnih baz. Rezultat tega je, da lahko z IDM sistemom centralno upravljamo z uporabniškimi identitetami.



Slika 3.3: Repozitorijske komponente

Med repozitorijske komponente spadajo tudi različne izpeljanke imenikov. Storitve, ki jih slednji nudijo, s skupnim terminom lahko imenujemo imeniške storitve, le-te obravnavam v nadaljevanju.

3.2.1. Imeniške storitve

Imeniška storitev *(ang. directory service)* je programska oprema, ki shranjuje, organizira in zagotavlja dostop do informacij v imeniku. [**32**]. Imeniške storitve so ena izmed tehnoloških predpostavk za delujoč IDM sistem, zato bom v tem podpoglavju predstavil nekatere pomembne zasnove in standarde imeniških sistemov.

3.2.1.1. Kaj je imenik?

V vsakdanjem življenju se pogosto srečujemo z različnimi vrstami imenikov *(ang. directory)*. Recimo s telefonskim imenikom (vključno z belimi in rumenimi stranmi), vodiči po televizijskih programih, raznimi nakupovalnimi katalogi itn. Takšne vrste imenikov lahko poimenujemo vsakdanji ali tudi nepovezani *(ang. offline)* imeniki. Iz zgoraj opisanih primerov je razvidno, da imeniki pomagajo ljudem najti stvari na način, da organizirajo ključne postavke in opise, ki so na voljo, v neko urejeno celoto.

V računalniškem svetu prav tako najdemo imenike, katerih namen in zgradba sta si podobna v mnogih pogledih, vendar z nekaj pomembnimi razlikami. Takšne imenike lahko poimenujemo, kar spletni *(ang. online)* imeniki. Takšni imeniki nudijo napredna in zahtevna iskanja zelo specifičnih informacij. Osnovne štiri značilnosti spletnih imenikov, po katerih se tudi najbolj razlikujejo od prej omenjenih nepovezanih imenikov, so: [**29**]

- dinamičnost,
- prilagodljivost,
- varnost in
- prilagojenost uporabniku

Pomembno je razumeti in razlikovati med različnimi vrstami imenikov. Kategorije, v katere lahko razdelimo imenike, obravnavam v nadaljevanju, in sicer v »poglavju 3.2.1.4. Vrste imeniških sistemov«.

Imeniški sistemi se pogosto zamenjujejo s podatkovnimi bazami. Res je, da imajo številne skupne lastnosti, kot so hitro iskanje in razširljiva shema. Vendar jih loči zelo pomembna lastnost. Imeniški sistemi so namreč optimizirani za bralne operacije, saj njihovo vsebino veliko bolj pogosto pregledujemo, kot spreminjamo. Bralne operacije so zato izredno hitre. Pri podatkovnih bazah pa se predpostavlja, da je frekvenca bralnih in pisalnih operacij približno enaka. Zato pri imeniških sistemih,

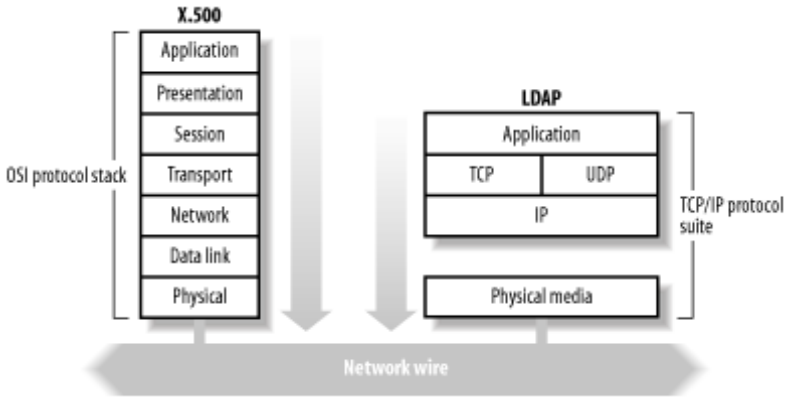
nekatere bistvene značilnosti podatkovnih baz, kot so recimo podpora transakcijam in zaklepanje podatkov, niso tako bistvene.[**4**]

3.2.1.2. X.500

X.500 je standard, ki zajema elektronske imeniške storitve. Standardiziran je bil pri organizaciji International Telecommunication Union - Telecommunication Standardization Sector *(krat. ITU-T)*. X.500 je pravzaprav niz standardov, čeprav izraz »X.500« na splošno uporabljamo v ednini, se kljub temu vedno sklicujemo na celotno zbirko standardov. Zbrane specifikacije v X.500 standardu opredeljujejo informacijsko strukturo imeniških storitev in protokole potrebne za dostop in upravljanje informacij, vsebovanih v imeniku.[**25**]

Standard X.500 si je prislužil naziv »težki«. Specificira namreč, da komunikacija med odjemalcem in strežnikom poteka z uporabo sedem slojnega protokolnega sklada modela OSI *(ang. Open System Interconnection)*. Natančneje, po dogovorjenem protokolu, imenovanem DAP *(ang. Directory Access Protocol)*. Kot protokol najvišjega aplikacijskega sloja v OSI modelu, mora DAP znati operirati tudi z vsemi ostalimi sloji v modelu. Podpora protokolnemu skladu OSI zahteva običajno večje zmogljivosti, kot so na voljo v majhnih okoljih. [**4**,**27**]

Zato je prišlo do razvoja preprostejšega protokola za dostop do imenika *(ang. Lightweight Directory Access Protocol, krat. LDAP)*.



Slika 3.4: X.500 preko OSI v primerjavi z LDAP preko TCP/IP [4]

X.500 je sčasoma postal zelo okoren, nudil je samo monoliten pogled na imenik, odjemalci so bili težki za realizacijo zato ga je v veliki meri nadomestil LDAP.[**6**]

Ker LDAP implementira zelo podoben podatkovni model kot standard X.500 je dodaten opis le-tega v poglavju »3.2.1.3. LDAP«. Več o standardih X.500 pa si bralec lahko prebere v [**25**].

3.2.1.3. LDAP

LDAP *(ang. Lightweight Directory Access Protocol)*. je omrežni protokol, ki določa načine za poizvedovanje in spreminjanje podatkov v imeniku. Besedo »lahki« oziroma »preprosti« je v svojem imenu pridobil iz dejstva, da gre pri tem protokolu v bistvu za prevetritev in poenostavitev različice imeniškega standarda X.500 in ima zato veliko značilnosti podedovanih od njega. Standard LDAP je opisan z naslednjimi štirimi modeli:

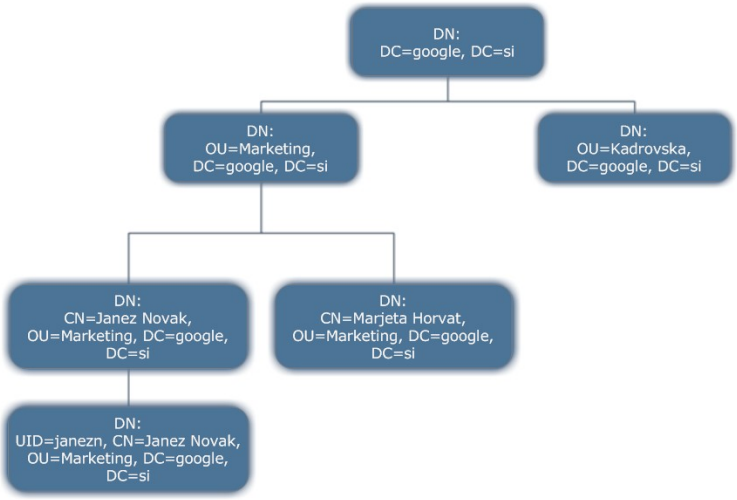
- *LDAP informacijski model:*

  Informacijski model definira tip podatkov oziroma osnovno enoto informacije, ki jo lahko shranimo v LDAP imenik in s katero lahko operiramo
- *LDAP imenski model:*

  Imenski model določa, da so vnosi urejeni v drevesno strukturo *(ang. Directory Information Tree, krat. DIT)*
- *LDAP funkcionalni model:*

  Funkcionalni model določa operacije, ki jih lahko izvajamo nad imenikom z uporabo LDAP protokola.
- *LDAP varnostni model:*

  Varnostni model določa načine povezovanja in avtentikacijske metode.



Slika 3.5: Primer LDAP drevesne strukture

Na »Sliki 3.5« je prikazan primer drevesne strukture LDAP. V primeru sem uporabil naslednje atribute:

- DC: Domain Component
- OU: Organizational Unit
- CN: Common Name

- UID: User ID
- DN: Distinguished Name

LDIF:

LDAP definira tudi t.i. LDAP Data InterChange Format *(krat. LDIF)*, ki je predpisani tekstovni format za opis informacije iz imenika. Format se uporablja tudi za prenos informacij iz enega imenika v drugega. Spodnji primer prikazuje opis nekega vnosa v imeniku z LDIF datoteko:[**27**]

```
dn: uid=Jnovak, ou=LKN, ou=TK, dc=fe, dc=uni-lj, dc=si
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Janez Novak
givenname: Janez
sn: Novak
uid: Jnovak
mail: janez@email.si
telephoneNumber: +386 1 5051473
```

3.2.1.4. Vrste imeniških sistemov

Dandanes obstaja nekaj osnovnih tipov imeniških sistemov, čeprav so meje med temi kategorijami pogosto zabrisane. Vsako vrsto imeniškega sistema lahko razvrstimo glede na tip objektov, ki jih vsebuje (obseg vsebine), ter glede na funkcionalnosti upravljanja in tip klientov (obseg storitev), ki jih podpira.[**25**] Na podlagi te ugotovitve lahko razdelimo izvedbe imeniških sistemov v šest podkategorij, ki jih predstavljam v nadaljevanju:

a.) Omrežno usmerjeni imeniki

Omrežno usmerjeni imeniki *(ang. Networking-focused directories)* so namenjeni podpori funkcijam omrežnih operacijskih sistemov, kot so uporabniški računi, varnost ter upravljanje omrežnih virov. Omrežno usmerjena imenika sta recimo Novell eDirectory in Microsoft Active Directory. Zgodnje implementacije omrežnih operacijskih sistemov so imele zelo preproste imenike, vendar so z razvojem integrirali različne vidike tehnologij opredeljenih v standardih X.500. [**25**,**29**]

b.) Splošno-namenski imeniki

Splošno-namenski imeniki *(ang. General-purpose directories)* služijo potrebam različnih aplikacij. Saj zagotavljajo najširšo paleto imeniških storitev in funkcionalnosti ter s tem podpirajo različne zahteve tako v poslovnem kakor tudi v omrežnem okolju. Trenutne izvedbe splošno-namenskih imenikov

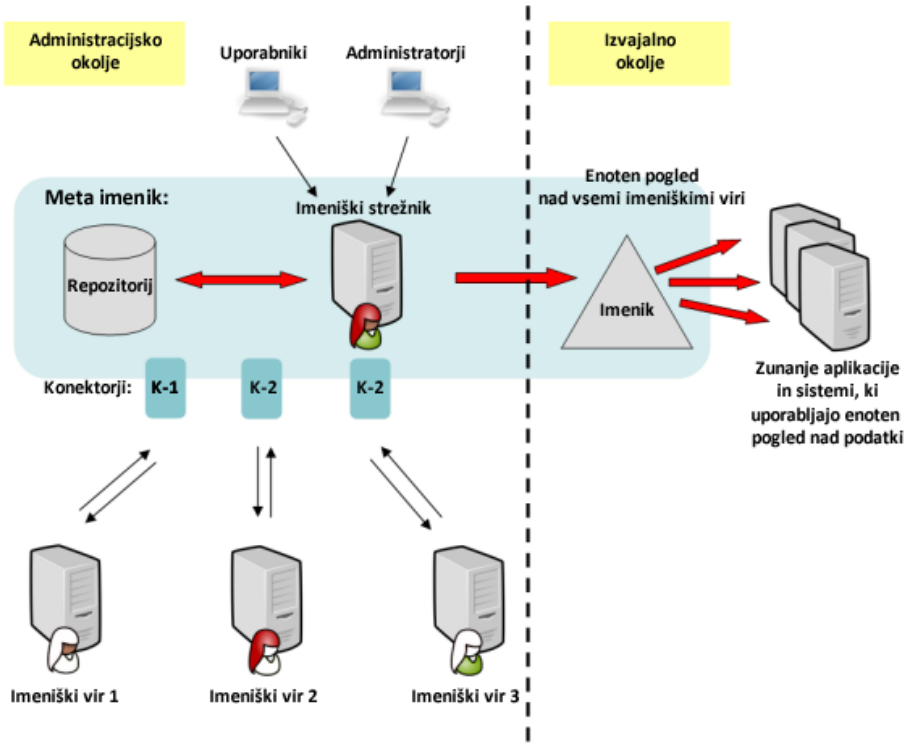
temeljijo na standardih X.500 in podpirajo protokole ter standarde, kot sta LDAP in sistem domenskih imen (*ang. Domain Name System, krat. DNS)*.[**25**]

c.) Aplikacijski imeniki

Aplikacijski imeniki *(ang. Application directories)* shranjujejo podatke o uporabnikih za specifične aplikacije. Najpogostejše področje uporabe te vrste imenikov je v izdelkih za skupinsko delo in sporočanje. Običajno so tako integrirani in vdelani v samo aplikacijo, da se pogosto sploh ne zavedamo, da v ozadju stoji imenik. Takšne vrste imenikov so npr. vgrajene v aplikaciji IBM Lotus Notes ter Microsoft Exchange. [**25**,**29**]

d.) Meta imeniki

Meta imeniki *(ang. Metadirectories)* zagotavljajo sredstva za upravljanje in povezovanje podatkov, shranjenih v različnih ter raznovrstnih imeniških virih. Meta imeniki uporabljajo programske agente oziroma konektorje za zbiranje podatkov iz različnih omrežij ter imenikov, ki se nato vključijo v sam meta imenik v različnem obsegu.



Slika 3.6: Tipična arhitektura meta imenika

Za njih je značilno, da so sposobni komunicirati z različnimi implementacijami imenikov ter podatkovnih baz, in s tem zagotavljajo funkcionalno interoperabilnost z različnimi omrežnimi operacijskimi sistemi ter aplikacijami. Njihov namen je zagotoviti enoten pogled nad podatki. Meta imeniki pogosto dvo ali več-smerno sinhronizirajo ter razvrščajo podatke z več imeniških virov, da bi

zgradili enoten - glavni ali nadimenik. Do katerega lahko potem dostopajo uporabniki, sistemi in storitve. Meta imenike si lahko predstavljamo kot prehodni korak k enotnemu, združenemu imeniku za shranjevanje podatkov.[**6**,**25**]. »Slika 3.6« prikazuje, na podlagi zgoraj podanega opisa, tipično arhitekturo meta imenika.

e.) Navidezni imeniki

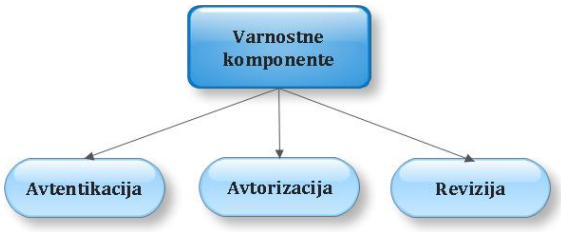
Navidezni ali virtualni imeniki *(ang. Virtual directories)* so v bistvu posebna vrsta meta imenikov. V obeh primerih imenika ustvarita enoten in neodvisen pogled na različne in raznovrstne implementacije že obstoječih imenikov - kot so: Active Directory, LDAP, relacijske podatkovne baze itn. Vendar so navidezni imeniki bistveno drugačni od meta imenikov v tem, da ne shranjujejo podatkov interno, ampak shranijo samo kazalce na dejanske podatke. Meta imeniki imajo vedno svoj repozitorij za shranjevanje podatkov, medtem ko navidezni imeniki zbirajo in shranjujejo podatke dinamično (v nekakšen predpomnilnik). To pomeni, da se dejanski podatki pridobijo iz drugih imenikov med samim procesiranjem.[**6**]. Pri meta imenikih so informacijski podatki različnih heterogenih sistemov med seboj fizično povezani, pri navideznih imenikih pa gre za logično povezavo, torej so podatki šibko sklopljeni.

f.) Ozko - namenski imeniki

Ozko-namenski imeniki *(ang. Specific-use directories)* niso vdelani v samo aplikacijo, ampak imajo ozko opredeljen namen shranjevanja informacij, ki ni razširljiv. Čeprav je lahko ta specifičen oziroma ozek namen karkoli. En primer takega imenika je DNS sistem, ki se uporablja za preslikavo med lažje zapomljivimi domenskimi imeni in težje zapomljivimi IP naslovi.[**25**,**29**] Na primer domena www.google.si ustreza IP naslovu 74.125.91.104.

3.3. Varnostne komponente

Varnostne komponente *(ang. Security components)* IDM sistemov se osredotočajo na informacijsko varnost. Omogočajo varen dostop do različnih informacijskih virov ter zagotavljajo integriteto podatkov.



Slika 3.7: Varnostne komponente

3.3.1. Avtentikacija

Avtentikacija ali overjanje *(ang. authentication)* je postopek ugotavljanja identitete, oziroma preverjanje pristnosti posameznika. V postopku avtentikacije preverjamo ali je identiteta veljavna v določenem kontekstu ali sistemu. Odjemalec *(ang. client)*, ki ga je potrebno overiti, je lahko končni uporabnik, stroj, storitev ali aplikacija. Postopek poteka tako, da se odjemalec najprej identificira oziroma predstavi. Sistem nato preveri ali so poverilnice *(ang. credentials)* odjemalca veljavne. Če so veljavne, se odjemalca smatra kot overjenega, oziroma pristnega (avtenticiranega). Z avtentikacijo potrdimo, da je identiteta aktivna in veljavna v okviru IDMS. [**6**]

Avtentikacija je ključnega pomena za procese avtorizacije in revizije. Če identiteta ni avtenticirana, potem celotna varnostna infrastruktura postane neučinkovita, ne glede na to kako dobra je. Ko je identiteta avtenticirana oziroma overjena, potrebuje še avtorizacijo za opravljanje nekega smiselnega dela.

Poverilnica dokazuje identiteto uporabnika na določeni ravni zaščite informacijskega sistema. Poverilnice predstavljajo fizično predstavitev identitete in z njimi povezanih pravic. Pri uporabi digitalne identitete za dostop do različnih virov mora poverilnica dokazati, da predstavljena identiteta res pripada tej osebi, sistemu ali procesu. [**6**]

Identifikacija omogoča IDM sistemu prepoznavanje digitalne identitete. To se zgodi z uporabo identifikatorja. Identifikator je lahko recimo ime. Identiteta se predstavi sistemu IDM z imenom, s tem se sklicuje na svojo digitalno identiteto. Naslednji korak IDM sistema je, da preveri pristnost te identitete, to se zgodi z avtentikacijo.

Do avtentikacije torej pride tako, da se uporabnik najprej identificira in nato predstavi svojo poverilnico. Sledi pregled nekaterih najpogostejših metod za avtentikacijo (poverilnic) v okviru IDM sistemov:

- *Gesla (ang. passwords):*
  Gesla so najcenejša in najpreprostejša rešitev za preverjanje pristnosti v sistemu IDM.
- *Avtentikacijski žetoni (ang. authentication tokens):*
  Delujejo kot elektronski ključ za dostop do nečesa. Poznamo jih v obliki pametnih kartic, žepnih računalnikov, USB žetonov itn.[**35**]
- *Infrastruktura javnih ključev (ang. Public Key Infrastructure, krat. PKI):*
  Digitalno potrdilo dokazuje identiteto lastnika javnega ključa. Infrastruktura javnih ključev omogoča izdajanje in upravljanje digitalnih potrdil oziroma certifikatov.

- *Biometrija (ang. Biometrics):*

  Biometrija je proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije in avtentikacije. Najbolj popularne oblike biometrije so: skeniranje očesne mrežnice ali šarenice, prstni odtisi, prepoznava glasu, prepoznava fotografij, itn.[**31**]

3.3.2. Avtorizacija

Avtorizacija ali pooblastitev *(ang. authorization)* je proces preverjanja, ali ima overjena stranka pravice za dostop do zahtevanega vira. [**6**]

Avtorizacijske komponente IDM sistemov nadzirajo identitete, kadar le-te dostopajo do informacijskih virov. V bistvu gre za preverjanje, kakšne so pravice identitete, ki zahteva dostop do vira oziroma storitve. Neki uporabnik ima lahko dostop do določenega informacijskega sistema glede na svoje pravice in dostopne politike organizacije. Dostop mu odobri ali zavrne prav avtorizacijska komponenta IDM sistema.

Odvisno od konteksta so »pravice« *(ang. Rights)* običajno analogne s pojmom »dostopne politike« *(ang. Access Policies)* ali »dostopna pravila« *(ang. Access Rules)*. Medtem ko so dovoljenja *(ang. Permissions)* analogna s seznamom za kontrolo dostopa *(angl. Access Control List, krat. ACL).* Običajna avtorizacijska dovoljenja v IDM sistemih so: branje *(ang. Read)* / pisanje *(ang. Write)* / izvajanje *(ang. Execute)* / pogled *(ang. View)* / tiskanje *(ang. Print)* / prestavljanje *(ang. Move)* / sprememba lastništva *(ang. Change Ownership)*. V implementacijah dovoljenj obstajajo velike razlike med IDM sistemi in ciljnimi oziroma upravljanimi sistemi. [**6**]

3.3.3. Revizija

Komponente za revizijo *(ang. Auditing)* omogočajo celovito revidiranje oziroma presojanje uporabniških profilov, spremljanje zgodovine sprememb in pravic uporabnikov, na ravni celotne organizacije. Revizija omogoča, da se varnostna tveganja odkrijejo zgodaj, tako da se lahko administratorji pravočasno in proaktivno odzovejo. Zmožnost, da lahko v vsakem trenutku pregledujemo stanja vseh dostopnih pravic uporabnikov, izboljša učinkovitost revizije in pomaga doseči skladnost z zakonskimi zahtevami ter predpisi.[**6**] Revizijske komponente zagotavljajo mehanizme za sledenje spremembam podatkov v repozitorijih (ustvarjanje, spreminjanje, dostopi, uporaba). S temi orodji je možno izvajati tudi forenzične analize, ki služijo ugotavljanju kdo in na kakšen način je zaobšel dostopne politike.[**11**]

3.4. Komponente življenjskega cikla

Slika 3.8: Komponente življenjskega cikla

Komponente življenjskega cikla *(ang. Lifecycle components)* imajo en glavni cilj, in sicer: popolno upravljanje, nadziranje in kontrolo življenjskega cikla posamezne identitete. Mednje štejemo oskrbovanje uporabnikov in pa orodja za zagotavljanje trajnosti *(ang. Longevity tools).*

3.4.1. Oskrbovanje uporabnikov

Za bolje razumevanje termina oskrbovanje uporabnikov *(ang. User provisioning)* bom navedel nekaj definiciji:

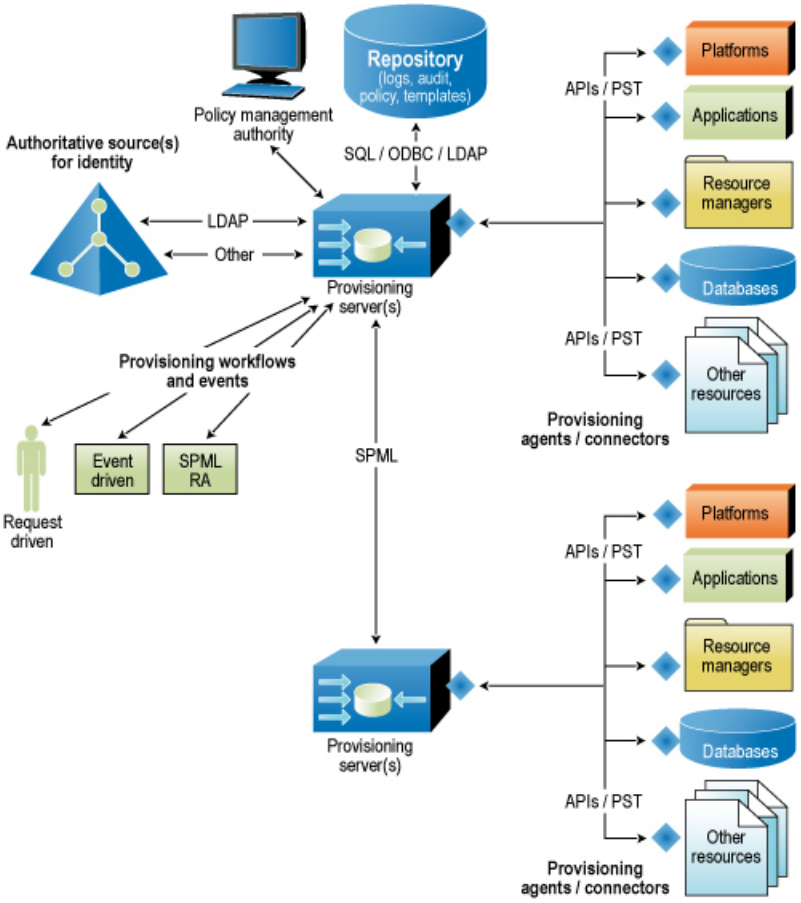
- Oskrbovanje uporabnikov lahko definiramo kot integriran nabor orodij za upravljanje življenjskega cikla uporabniških pravic.[**3**]
- Oskrbovanje uporabnikov je funkcija IDMS, ki ustvarja identitete v drugih »ciljnih« sistemih in odstranjuje identitete iz ciljnih sistemov, ko le-te niso več potrebne. Oskrbovanje uporabnikov se nanaša tako na storitve, ki jih nudi IDMS, kakor tudi na postopke ustvarjanja, dodajanje ali odstranjevanje identitet.[**6**]
- Oskrbovanje uporabnikov prinaša zmogljivosti za upravljanje digitalnih identitet uporabnikov preko sistemov, aplikacij in virov.[**23**]

Oskrbovanje bi lahko opisali kot proces dodeljevanja delovnih sredstev uporabniku za potrebe izvajanja delovnega procesa. V bistvu gre za avtomatizacijo vseh postopkov in orodij za upravljanje življenjskega cikla identitete. Postopki oskrbovanja uporabnikov vključujejo:

- Ustvarjanje enoličnega identifikatorja za identiteto
- Povezovanje z avtentikacijskimi komponentami
- Nastavitev in spreminjanje vsebine ter privilegijev identitete
- Izbris identitete [**11**]

3.4.1.1. Sestavni deli sistemov za oskrbovanje uporabnikov

V pričujočem poglavju bom predstavil nekatere poglavitne komponente sistemov za oskrbovanje uporabnikov. »Slika 3.9« prikazuje generični arhitekturni model sistemov za oskrbovanje uporabnikov. Končne implementacije sistemov se v praksi razlikujejo od tega modela glede na filozofijo proizvajalca sistema, ekspertizo, izkušnje ter pristop.[**3**]



Slika 3.9: Generični arhitekturni model sistemov za oskrbovanje uporabnikov[3]

a.) Strežnik za oskrbovanje uporabnikov

V srcu vsakega sistema za oskrbovanje uporabnikov je strežnik *(ang. The Provisioning Server)*. V strežniku se obdelujejo pravila, delovni tokovi, poročila ter varnostne politike. Strežnik lahko predstavlja tudi jedro oziroma središče arhitekture IDM sistema, ki se nato preko vmesnikov usklajuje z drugimi poglavitnimi komponentami. Takšen - osrednji arhitekturni model je bolj tipičen za sisteme, ki so bili razviti ali pa so organsko rasli znotraj ponudbe kakega izmed proizvajalcev. Za razliko od sistemov proizvajalcev, ki so svoje sisteme za oskrbovanje uporabnikov dopolnjevali s prevzemi konkurentov in so še vedno v fazi integracije.[**3**]

b.) Vmesniki

Vmesniki *(ang. Interfaces)* so potrebni za izvajanje sistemskih administracijskih funkcij, ki ustvarjajo in upravljajo okolje za oskrbovanje uporabnikov. Ločen nabor vmesnikov je rezerviran za uporabniške samopostrežne funkcije in za vodje posameznih poslovnih dejavnosti, katerim so delegirane določene administracijske naloge.

Sistemski administratorji potrebujejo enostavna, a hkrati napredna orodja za:

- vzpostavitev povezav z avtoritativnimi identitetnimi viri,
- kreiranje delovnih tokov,
- nastavitve revizijskega nadzora,
- vzpostavljanje varnosti,
- avtomatizacijo postopkov
- integracijo s ciljnimi sistemi

Delegirana administracija je pomembna funkcionalnost za organizacije, ki breme upravljanja z uporabniki selektivno porazdeli neposredno na posamezne osebe in skupine, ki so najbolj primerne za izvajanje tovrstnih organizacijskih storitev. Takšen sistem za oskrbovanje uporabnikov mora imeti vmesnike, ki omogočajo preproste in ustrezne možnosti nastavljanja varnostnih ukrepov za vsakega pooblaščenega administratorja.

Samopostrežni administracijski vmesniki omogočajo dodatno razbremenitev administratorjev, saj enostavna opravila kot je npr. ponastavitev gesla, prelagajo na vsakega posameznika znotraj organizacije. Številne organizacije preferirajo, da tudi zahteve za dostop do posameznih virov, uporabniki oddajajo preko samopostrežniških administracijskih vmesnikov. Pooblaščeni administratorji pa jih preko istih vmesnikov odobravajo. [**3**]

c.) Delovni tokovi in obdelava dogodkov

Z delovnimi tokovi *(ang. Workflow)* in pravili za obdelavo dogodkov *(ang. Event Processing rules)* se usklajuje in orkestrira procese oskrbovanja uporabnikov za nove člane organizacije (npr. nove zaposlitve), morebitne statusne spremembe (npr. napredovanje) in tiste, ki organizacijo zapuščajo *(ang. deprovisioning)*.[**3**]

d.) Agenti in konektorji

Agenti oziroma konektorji *(ang. Agents / Connectors)* zagotavljajo nujno povezavo med strežnikom za oskrbovanje uporabnikov in informacijskim sistemom ali poslovno aplikacijo, ki jo želimo upravljati. Termin agent je sopomenka izrazu konektor. Nekateri ponudniki IDM izdelkov razlikujejo med

»konektorji«, ki opravljajo akcije v imenu sistema in/ali uporabnika in »adapterji«, ki predstavljajo predloge za pristop k povezovanju IDMS, za različne ciljne sisteme, ki vsebujejo podatke (kot so podatkovne baze in imeniške storitve). [**3**,**6**]

Nekateri agenti podpirajo napredno dvosmerno komunikacijo in so sposobni prenašati spremembe narejene na ciljnih sistemih (virih) nazaj v strežnik za oskrbovanje uporabnikov. Večina današnjih agentov podpira osnovne funkcije upravljanja uporabniških računov. Upravljanje bolj prefinjenih funkcij ciljnega sistema, kot je npr. urejanje skupinskih varnostnih pravic dostopa, pa se močno razlikuje med posameznimi proizvajalci IDM sistemov. Vodilni proizvajalci IDM sistemov tako za rešitev specifičnih zahtev, ponujajo močna orodja za razvoj konektorjev, narejenih po meri.[**3**]

Vrste agentov / konektorjev:

V preteklosti se je razlika med dvema glavnima vrstama agentov *(ang. Agent Types)* uporabljala v tržne namene kot dejavnik konkurenčnosti med različnimi ponudniki. Danes skoraj vsak ponudnik podpira oba tipa agentov, oddaljene *(ang. remote agents)* ter lokalne *(ang. local agents).* Preference in zahteve kupcev pa odločajo, kje bodo le ti nameščeni. Tretja vrsta agentov, ki temelji na jeziku Service Provisioning Markup Language *(krat. SPML)* bi se naj uveljavila v prihodnosti, ko bodo proizvajalci in ponudniki sprejeli standard. »Tabeli 3.1 in 3.2« prikazujeta nekatere prednosti in slabosti pri implementaciji lokalnega oziroma oddaljenega agenta.[**3**]

Lokalni agenti	
Prednosti:	**Slabosti:**
▪ običajno nudijo boljše temelje za porazdeljene sisteme ▪ boljša izraba pasovne širine potrebne za komunikacijo s strežnikom za oskrbovanje uporabnikov ▪ detekcija sprememb poteka lokalno (npr. zaznava spremembe gesla, sinhronizacija gesla s strežnikom) , zaradi tega dvosmerna komunikacija lahko poteka skoraj v realnem času	▪ bolj kompleksni od oddaljenih agentov, ▪ namestitev morda potrebna preko ciljnega sistema ▪ pri nadgradnji ciljnega sistema lahko pride do težav s povezljivostjo, če ni tudi nadgradnje konektorja

Tabela 3.1: Prednosti in slabosti lokalnih agentov

Oddaljeni agenti	
Prednosti:	**Slabosti:**
▪ preprostejša implementacija ▪ manj občutljivi na nadgradnje ciljnega sistema	▪ pri nekaterih implementacijah je funkcionalnost omejena na enosmerno ali potisno *(ang. push)*

▪ centralizirajo administrativne in nadzorne funkcije na strežniku za oskrbovanje uporabnikov in tako poenostavljajo arhitekturo sistema	komunikacijo s ciljnim sistemom ▪ zaradi enosmerne komunikacije so takšni sistemi manj sposobni pri detekciji sprememb in spremljanju dogodkov na ciljnih sistemih v realnem času ▪ tipično ne zmorejo zagotoviti dvosmerne sinhronizacije gesel

Tabela 3.2: Prednosti in slabosti oddaljenih agentov

e.) Repozitoriji za storitve oskrbovanja uporabnikov

Sistemi za oskrbovanje uporabnikov uporabljajo imeniške in podatkovne repozitorije za shranjevanje identitetnih podatkov, informacij o konfiguracijah, varnostnih politik, revizijskih evidenc ter ostalih informacij. Sistemi nameščajo in uporabljajo repozitorije na različne načine. Nekateri znajo za svoje delovanje uporabiti obstoječe imeniške sisteme ali podatkovne baze, ki jih potrebujejo za shranjevanje informacij. Spet drugi zahtevajo namestitev namenskega repozitorija za skladiščenje podatkov, potrebnega za storitve oskrbovanja uporabnikov.

Trenutno mnogo proizvajalcev podpira navidezne imenike, kjer so v strežniku za oskrbovanje uporabnikov shranjeni samo metapodatki o uporabniških identitetah, dejanski podatki pa se pridobijo iz avtoritativnih sistemov med samim procesiranjem.

Drug pristop je shranjevanje uporabniških identitet v osrednjem repozitoriju samega sistema. To zahteva sinhronizacijo oziroma uskladitev vseh podatkov, na način, da je osrednja kopija podatkov vedno najnovejša. Shranjevanje vseh uporabniških podatkov na enem mestu omogoča proizvajalcem, da pospešijo obdelavo, analizirajo podatke za razčlenitev vlog *(ang. separation of duties)* in omejitev, ter lažje poročajo o zbranih podatkih.

Ponudniki, ki uporabljajo centraliziran pristop shranjevanja podatkov, imajo še vedno možnost, da zahtevajo uporabniške podatke med procesiranjem, vendar je to prej izjema kot pravilo, saj je večina podatkov shranjena v osrednjem repozitoriju.[**3**]

f.) Avtoritativni identitetni viri

Pomembno je, da poznamo pojem avtoritativni identitetni vir. Avtoritativni identitetni vir *(ang. Authoritative Identity Sources)* je običajno en izmed oddaljenih virov podatkov, ki so v kadrovski službi. Tam hranijo večino informacij o zaposlenih v organizaciji. Avtoritativni se imenuje zato, ker gre za podatke, ki predstavljajo primarni vir informacij. Vsi ostali viri podatkov so podmnožice

avtoritativnega vira podatkov. Kadar avtomatizirani sistemski prožilci zaznajo spremembo v avtoritativnem viru, le-to pošijejo tudi v strežnik za oskrbovanje uporabnikov.

Sistemski viri so povezani s strežnikom za oskrbovanje uporabnikov na številne različne načine, vključno s prenosom nepovezanih datotek *(ang. flat file transfers)* ter enosmerno in dvosmerno povezavo. Za kadrovske sisteme je še vedno v navadi, da ustvarjajo nepovezane datoteke sprememb uporabnikov in z njimi povezanih atributov, ki jih nato obdeluje strežnik za oskrbovanje uporabnikov. Kljub učinkovitosti, takšna paketna metoda obdelave ne zagotavlja posodobitve podatkov o dostopih uporabnikov v realnem času.

Večina oskrbovalnih strežnikov zagotavlja konektorje ali poslušalce, ki se namestijo na kadrovske informacijske sisteme. Tam zajemajo vse spremembe uporabnikov in jih nemudoma posredujejo strežniku za oskrbovanje uporabnikov. Uveljavljena kadrovska informacijska sistema, kot sta SAP in PeopleSoft, sta podprta na tak način. Nekatera podjetja omogočajo celo dvosmerno povezljivost s kadrovskim sistemom. Dvosmerna povezljivost se uporablja predvsem pri posodobitvah sistemskih atributov kadrovskega sistema, ki so lahko posledica sprememb v drugih avtoritativnih sistemih, ali pa preprosto za upravljanje in dostop do kadrovske aplikacije.[**3**]

g.) Upravljanje gesel

Vsi današnji proizvajalci sistemov za oskrbovanje uporabnikov zagotavljajo upravljanje gesel *(ang. Password Management)* na enega izmed dveh načinov: ponastavitev ali sinhronizacija gesla. Mnogo jih ponuja obe zmogljivosti. Večina proizvajalcev nudi tudi samopostrežno ponastavitev gesla, ne pa tudi samodejne sinhronizacije gesla na vse sisteme.

Organizacije potrebujejo tudi netipične uporabniške vmesnike za samopostrežno ponastavitev gesla. Kajti uporabnik, ki se je zaklenil iz omrežja in nima dostopa do spletnega brskalnika, ne bo mogel dostopati do spletnega obrazca, z namenom ponastavitve svojega gesla. Nekateri proizvajalci v svoje sisteme zato vključujejo telefonske vmesnike, ki omogočajo ponastavitev gesel ali pa kakšen drug podoben pristop, ki rešuje uporabnike brez dostopa do spletne ponastavitve gesla.[**3**]

h.) Revizija upravljanja identitet

Skladnost z regulativnimi zahtevami je eden izmed poglavitnih poslovnih gonilnikov pri vpeljavi sistemov za oskrbovanje uporabnikov v organizacijo. Zato so proizvajalci v sisteme vpeljali funkcionalnosti revizijskih storitev upravljanja identitet *(ang. Identity Audit, krat. IDA)*, ki zagotavljajo zakonsko usklajeno rabo revizijske sledljivosti življenjskega cikla identitet.

Nekateri proizvajalci ponujajo IDA sisteme kot samostojne izdelke, medtem ko jih drugi vgrajujejo, kot modul, v sisteme za oskrbovanje uporabnikov. Večina sistemov za oskrbovanje uporabnikov že sama po sebi omogoča izdelavo poročil v slogu kdo, ima dostop do česa, in kdo je izvedel neko dejanje na določenem viru, ter katere pravice so neskladne z vlogo uporabnika (pretirani privilegiji). Vendar IDA sistemi močno presegajo le golo funkcionalnost poročanja, saj revizorja opremijo tako s preventivnimi kakor tudi z detektivskimi funkcionalnostmi nadzora.

IDA podpira zaščitne ukrepe, ki omogočajo organizacijam, da določijo varnostno politiko nadzora dostopa, kot so npr. politika razčlenjevanja vlog *(ang. Separation of duties, krat. SOD)*. Te varnostne politike se nato povežejo na ravni celotne organizacije, s primarnim ciljem - zagotavljanje notranje kontrole.

IDA omogoča revizijo dostopov in potrjevanja, usklajevanja pravic uporabnikov v primerjavi s tem, kar narekuje varnostna politika organizacije ter revizijo mirujočih ali mrtvih uporabniških računov.[**3**]

i.) Upravljanje vlog

Upravljanje vlog *(ang. Role Management)* predstavlja mehanizem za upravljanje korelacije med poslovnimi pristojnostmi in sredstvi potrebnimi za njihovo zadovoljitev. V praksi so odgovornosti običajno opisane kot poslovne vloge, sredstva so pa običajno združena v ustreznih uporabniških vlogah *(ang. IT roles)*. ustvarjanje in upravljanje teh vlog in z njimi povezanih politik so domena sistemov za obvladovanje poslovnih pravil *(ang. Enterprise Role Management, krat. ERM).*

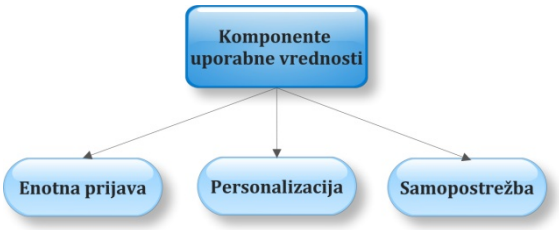
Sistemi za oskrbovanje uporabnikov se običajno navezujejo kar na uporabniške vloge, prevzete iz ERM sistemov. Oskrbovanje uporabnikov je namreč bolj osredotočeno na zagotavljanje dostopa do virov in ni primerno za odgovore na vprašanja v slogu, zakaj je določen dostop odobren ali zavrnjen. Iz te perspektive je vidna sinergija med oskrbovanjem uporabnikov in upravljanjem z vlogami. Upravitelj vlog namreč zajema podatke o tem, komu je bila dodeljena vloga, kakšni so pogoji za njeno dodelitev ter katera sredstva so bila dodeljena tej vlogi. Takšna rešitev zadostuje tako potrebam administratorjev in revizorjev, kakor tudi za upravljanje poslovnih procesov.[**3**]

3.4.2. Orodja za zagotavljanje trajnosti

Orodja za zagotavljanje trajnosti ustvarjajo evidenco zgodovine posamezne identitete skozi čas. To omogoča popolno časovno pregledovanje razvoja identitete. Orodja za zagotavljanje trajnosti so povezana s konceptom potrjevanja - sposobnost določevanja katera identiteta je imela dostop do katerega vira in v katerem časovnem okviru (ne glede na to, ali je bil izveden dostop, kar je predmet revizije).[**12**]

3.5. Komponente uporabne vrednosti

Komponente IDM sistema, ki jih imenujemo s skupnim imenom komponente uporabne vrednosti *(ang. Consumable value components)* se nanašajo na tri generične tipe tehnologij, in sicer: Enotna prijava *(ang. Single Sign-On, krat. SSO),* Personalizacija *(ang. Personalization)* in Sampostrežba *(ang. Self Service).*



Slika 3.10: Komponente uporabne vrednosti

3.5.1. Enotna prijava

Mnogo uporabnikov porabi ogromno časa samo z dostopanjem do različnih aplikacij in sistemov. Študije kažejo, da povprečni zaposleni porabi kar 44 ur na leto samo zato, da se prijavlja v različne informacijske sisteme. To je malenkost več kot teden dni dela povprečnega zaposlenega.[**24**] Enotna prijava omogoča uporabniku, da izvaja primarno overjanje samo enkrat, potem pa ima dostop do celotnega nabora aplikacij in informacijskih sistemov, ki so vključene v okolje IDM sistema. [**12**] S tem se čas, ki se zapravlja s prijavljanjem v različne sisteme zmanjša za faktor štiri.[**24**] Poveča se tudi varnost celotnega IT okolja, saj si uporabnik mora zapomniti samo eno geslo, ki je lahko zato bolj kompleksno.

SSO strežnik shranjuje gesla za vsak sistem, do katerega ima uporabnik dostop. Uporabnik je overjen s strani SSO strežnika samo enkrat, na primer pri prijavi v omrežje. Ko uporabnik želi uporabljati neko aplikacijo in le-ta zahteva poverilnice, bo SSO strežnik prestregel to zahtevo in odgovoril aplikaciji v imenu uporabnika. Več o tem lahko zainteresiran bralec najde v [**24**].

3.5.2. Personalizacija

Orodja za personalizacijo oziroma prilagajanje omogočajo upraviteljem, da uporabniške vmesnike s katerimi prihajajo v stik zaposleni, prilagodijo tako, da nudijo enoten videz na ravni celotne organizacije. S tem se lahko poenostavi uporabniški vmesnik in uvajanje uporabnikov v nov sistem je zaradi prilagoditve mnogo lažji.[**11**]

3.5.3. Samopostrežba

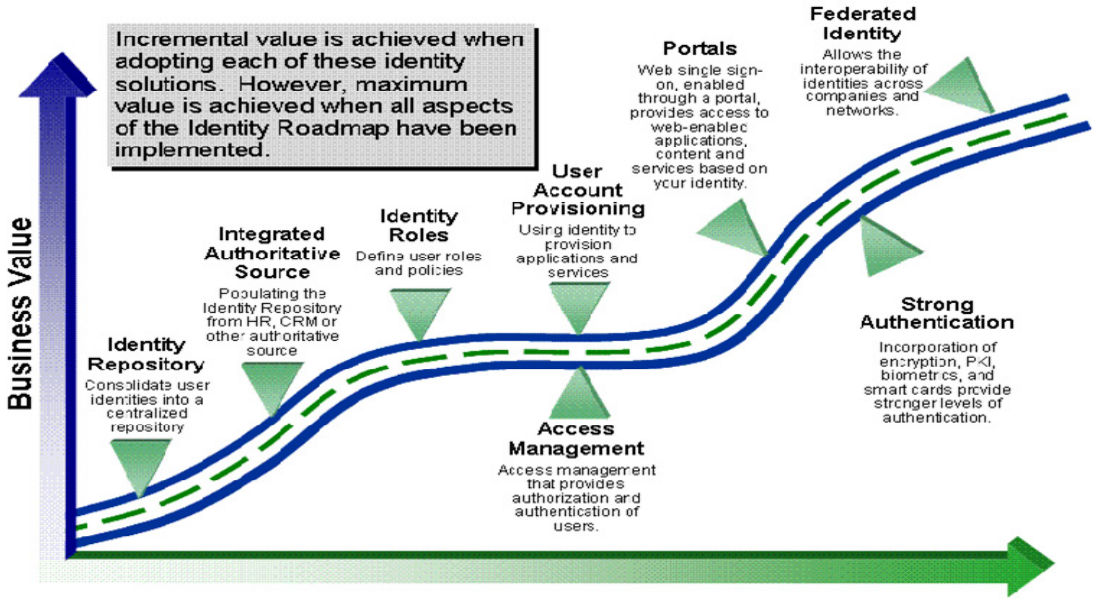
Samopostrežba omogoča uporabnikom, da se sami prijavijo za dostop do poslovnih storitev. Omogoča tudi urejanje lastnega uporabniškega profila, brez posredovanja administratorjev. Uporabniki lahko upravljajo tudi s poverilnicami za overjanje oziroma avtentikacijo: dodeljujejo in ponastavljajo gesla, zahtevajo digitalne certifikate, itn. Samopostrežne storitve zmanjšujejo stroške poslovanja, kakovost storitev za stranke dvigujejo na višjo raven, izboljšajo pa tudi skladnost in točnost informacij.[**11**]

Poglavje 4:

SISTEMI ZA UPRAVLJANJE IDENTITET

4.1. Prednosti uporabe sistemov za upravljanje z digitalnimi identitetami

V tem poglavju bom na kratko opisal nekatere poslovne prednosti, ki jih prinese uporaba sistemov za upravljanje digitalnih identitet organizaciji v praksi. Pri tem sem opiral na vir [**24**].



Slika 4.1: Načrt implementacije IDM sistemov [7]

IDM sistemi so veliko več, kot samo tehnične rešitve upravljanja digitalnih identitet. Imajo tudi realno poslovno vrednost. Kot je razvidno iz »Slike 4.1«, je največja poslovna vrednost v praksi dosežena z implementacijo vseh komponent IDM sistemov, ki so opisane v »poglavju 3.« tega dela.

Spodnji seznam prikazuje nekatere lastnosti IDM sistemov, ki zmanjšujejo stroške, namenjene za informatiko:

- Centralizirano upravljanje uporabnikov omogoča zmanjševanje administracijskih stroškov. Dostop do informacijskih virov za novega zaposlenega je s pomočjo avtomatizacije oskrbovanja uporabnikov omogočen v nekaj minutah ali urah, namesto v dnevih.
- Z uporabo meta imenikov ali navideznih imenikov se zmanjšajo stroški administriranja in iskanja informacij.
- Študije kažejo, da povprečni zaposleni porabi kar 44 ur na leto samo zato, da se prijavlja v različne informacijske sisteme. To je malenkost več kot teden dni dela povprečnega zaposlenega. Z implementacijo enotne prijave se čas, ki se zapravlja s prijavljanjem v različne sisteme zmanjša za faktor štiri.
- Samopostrežno upravljanje zmanjšuje stroške poslovanja, ker se s tem zmanjša obremenjenost administracijskega in tehničnega osebja. Uporabniki lahko sami opravljajo preprosta administracijska opravila, kot je recimo ponastavitev gesla.
- Federacija pomeni delitev identitet uporabnikov s tretjimi pogodbenimi strankami z namenom združevanja storitev. To seveda vodi k zmanjševanju stroškov, saj se breme upravljanje identitet deli s partnerji.

Naslednji seznam ponuja nekatere koristi, ki jih občutijo končni uporabniki informacijskih sistemov in aplikacij organizacije (zaposleni, stranke, dobavitelji):

- Enotna prijava omogoča, da se uporabniki prijavijo le enkrat in že imajo dostop do aplikacij in informacijskih sistemov, ki uporabljajo to funkcionalnost. Z uporabo enotne prijave si mora uporabnik zapomniti samo eno geslo, ki je lahko zato bolj kompleksno (večja varnost). S tem odpade lepljenje gesel po delovnih mizah, monitorjih in ostalih delovnih površinah, kot je to žal v navadi po organizacijah.
- Personalizacija vmesnikov s katerimi prihajajo v stik zaposleni, omogoča, da se uporabniški vmesniki prilagodijo tako, da nudijo enoten videz na ravni celotne organizacije.
- Samopostrežne storitve omogočajo uporabnikom, da se sami prijavijo za dostop do informacijskih virov. Med drugim nudijo tudi urejanje lastnega uporabniškega profila, brez

posredovanja administratorjev. Uporabniki lahko ponastavljajo gesla, zahtevajo digitalne certifikate, itn.

Ena izmed poglavitnih prednosti vpeljave IDM sistema v organizacijo je pa seveda izboljšana varnost na ravni celotne organizacije ter skladnost s predpisi in zakoni.

- Zaščita informacijskih virov z uporabo avtentikacije, avtorizacije, infrastrukture javnih ključev povečuje varnost.
- S pomočjo nastavljivih varnostnih politik zmanjšujemo varnostna tveganja in preprečujemo nepooblaščene dostope do virov.
- Sistemski dnevniki lahko beležijo celoten življenjski cikel posamezne identitete, kar omogoča revizijo dostopov in s tem skladnost s predpisi in zakoni.
- Hitrejše in preprostejše odkrivanje zlorab, nepravilnih informacij oz. pravic uporabnika, onemogočanje dostopa nekdanjih zaposlenih do informacijskega sistema, itn.
- Možnosti hitrega odziva pri zaznanih varnostnih problemih in incidentih.

Varnostne kontrole upravljanja dostopov nudijo možnost oddaljenega dostopa, s tem je mogoče delo od doma.

4.2. Vrste sistemov

4.2.1. Celoviti sistemi za upravljanje identitet

Sistemi za upravljanje z digitalnimi identitetami *(ang. Identity Management Systems, krat. IDMS/IMS)* so celovito ogrodje oziroma programski paket, ki običajno obstaja znotraj neke določene administrativne meje, kot je recimo domena ali organizacija. To ogrodje zagotavlja upravljanje z dostopi in avtorizacijami, revizijo, poročanje, močno avtentikacijo, federacijo, upravljanje življenjskega cikla digitalnih identitet, vmesnike za različne ciljne sisteme ter imeniške storitve. Upoštevati je treba, da se IDMS nanaša na infrastrukturo, ogrodje, programsko opremo, strežnike, omrežje in sisteme, ki skupaj zagotavljajo celovite IDM storitve.[**6**]

Celoviti sistemi za upravljanje identitet *(ang. Identity And Access Management Suite)* so za razliko od parcialnih sistemov, sestavljeni iz med seboj popolnoma usklajenih, pred-vgrajenih komponent enega proizvajalca. S tem se poenostavlja integracija in namestitev IDM sistema, ki lahko dramatično zmanjša stroške uvajanja takega sistema v organizacijo.

Privzamemo lahko, da celoviti sistemi za upravljanje identitet podpirajo večino ali pa kar vse izmed komponent, ki so bile predstavljene v »poglavju 3.« tega dela in morda še nekatere specifične funkcije, prevzete iz parcialnih sistemov.

Nekateri proizvajalci nudijo svoje rešitve iz celovitih sistemov, kot posamezne komponente. V tem primeru govorimo že o parcialnih sistemih za upravljanje identitet. Primerni so za tista podjetja, ki se želijo osredotočiti samo na specifična področja v okviru IDM.

4.2.2. Delni sistemi za upravljanje identitet

Delni sistemi za upravljanje identitet *(ang. Point Identity And Access Management Products)* se običajno osredotočajo samo na specifičen segment infrastrukture IDM. Za doseganje enake funkcionalnosti, kot pri celovitih sistemih je potrebno parcialne sisteme med seboj integrirati in uskladiti, kar posebej pri komponentah različnih proizvajalcev lahko povzroča nemalo preglavic.

Za vsako komponento iz IDM ogrodja, opisano v poglavju 3. tega dela obstaja delni sistem kot samostojna rešitev.

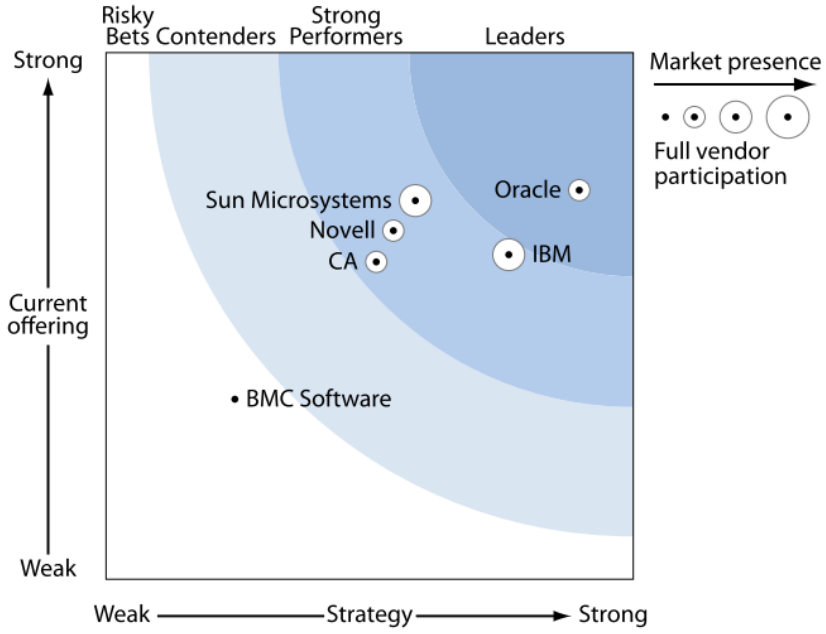
4.3. Pregled celovitih sistemov za upravljanje identitet

V tem podpoglavju sledi pregled trenutno vodilnih ponudnikov na trgu celovitih IDM sistemov. Celovite sisteme vodilnih proizvajalcev na trgu sem identificiral s pomočjo poročila svetovalsko-analitskega podjetja »Forrester Research« [**8**].

Pregled celovitih rešitev na trgu IAM odraža njeno zgodovino. Vsak izmed segmentov trga je namreč nastal iz ločenih oziroma parcialnih sistemov, kot lasten sistem za reševanje precej različnih potreb. Proizvajalci so sčasoma začeli prepoznavati temeljno vlogo, ki jo ima identiteta v celotnem kontekstu. S prevzemi parcialnih sistemov drugih proizvajalcev in lastnim razvojem so sčasoma nastali celoviti sistemi za upravljanje identitet, kot razširitev svoje temeljne poslovne strategije posameznega proizvajalca.[**8**]

Primarni selekcijski kriterij za sodelovanje v raziskavi »Forrester-ja« je bil, da proizvajalec premore lastno linijo IAM izdelkov na ključnih področjih upravljanja identitet. Le-ta so naslednja: oskrbovanje uporabnikov, enotna prijava in pa federacija.

»Slika 4.2« prikazuje vodilne proizvajalce celovitih sistemov za upravljanje identitet. Evalvacijska merila za uvrstitev na lestvico si zainteresiran bralec lahko pogleda v [**8**], tukaj bom samo komentiral rezultate iz poročila, prej omenjenega vira.



Slika 4.2: Vodilni proizvajalci celovitih sistemov za upravljanje identitet [8]

Kot je razvidno iz »Slike 4.2«, se je podjetje Oracle uveljavilo kot vodilni proizvajalec celovitih sistemov za upravljanje identitet. Kot močni proizvajalci na trgu so zastopana podjetja: »IBM«, »Sun«, »Novell«, in »CA«. Sodeč po analizah »Forrester-ja« proizvajalec »BMC Software« precej zaostaja za ostalimi ponudniki s svojim IAM portfeljem. V analizi sta manjkali podjetji »HP« in »Microsoft«, prvo se je odločilo izstopiti iz IAM trga in nehalo razvijati nove verzije IDM sistemov. »Microsoft« pa ni bil vključen v raziskavo zaradi nekaterih pomanjkljivosti, ki jih ima v svojem IAM portfelju in ne ustrezajo merilom za vključitev v raziskavo podjetja »Forrester«.

4.4. Pregled sistemov za oskrbovanje uporabnikov

Sistemi za oskrbovanje uporabnikov so v bistvu delni sistemi za upravljanje identitet in kot takšni podmnožica celovitih sistemov za upravljanje identitet. Zato ni presenetljivo, kot bo razvidno iz nadaljevanja poglavja, da so med vodilnimi izdelovalci sistemov za oskrbovanje uporabnikov skoraj ista podjetja kot na trgu celovitih rešitev za upravljanje identitet iz prejšnjega podpoglavja.

S pomočjo sistemov za oskrbovanje uporabnikov rešujejo organizacije potrebe po ustvarjanju, spreminjanju, onemogočanju ter izbrisu uporabniških identitet znotraj heterogene IT infrastrukture.

Le-ta vključuje operacijske sisteme, podatkovne baze, imeniške sisteme, poslovne aplikacije in varnostne sisteme. Gartner razlikuje pojma »oskrbovanje uporabnikov« in »upravljanje identitet«. Oskrbovanje uporabnikov je podskupina sistemov za administriranje identitet., ki so podskupina širše krajine IAM izdelkov. [**10**]

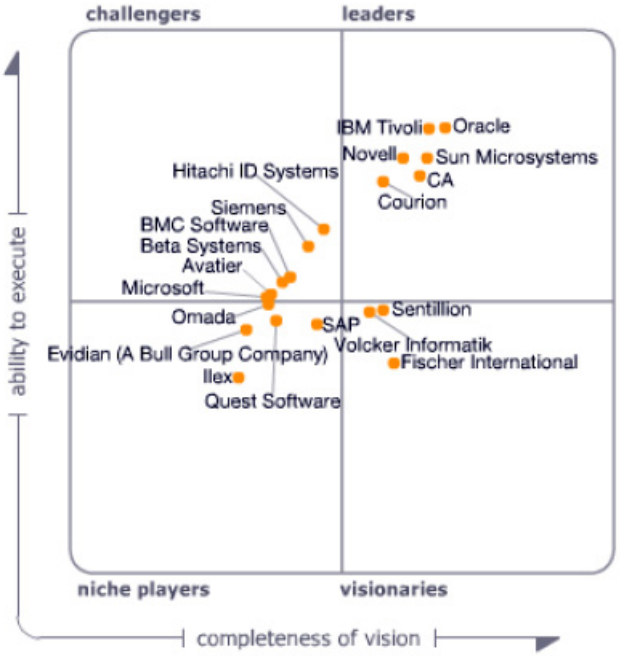
Sistemi za oskrbovanje uporabnikov so glavni pospeševalnik pri administriranju identitet. Pri pregledu trga sem si pomagal z zadnjim (September 2009) poročilom, uveljavljenega analitsko-svetovalnega podjetja na področju računalništva in informatike - »Gartner« [**10**]. Analitiki pri Gartnerju uvrščajo proizvajalce sistemov za oskrbovanje uporabnikov v magični kvadrant, glede na zmogljivost in kakovost rešitve, izkušnje strank in celostno vizijo proizvajalca. Podrobna merila, ki vplivajo na uvrstitev posameznih proizvajalcev si bralec lahko ogleda v [**10**].

Sistemi za oskrbovanje uporabnikov implementirajo nekatere ali pa vse izmed v nadaljevanju naštetih funkcionalnosti:

- Delovne tokove, proces za preverjanje in odobritve - (ang. Workflow and approval processes)
- Upravljanje gesel (z možnostjo samopostrežne ponastavitve) - (ang. Password management)
- Upravljanje drugih poverilnic - (ang. Other credential management)
- Upravljanje življenjskega cikla vloge uporabnika - (ang. Role life cycle management)
- Administracija uporabniških dostopov (z možnostjo samopostrežne administracije) - (ang. User access administration)
- Administracija informacijskih virov (z možnostjo samopostrežne administracije) - (ang. Resource access administration)
- Osnove IAM obveščanja (analiza, revizija, poročanje) - (ang. Basic IAM intelligence - analytics, auditing, reporting)

Kot je razvidno iz »Slike 4.3«, Gartner proizvajalce diferencira v štiri skupine:

- Vodilni proizvajalci *(ang. leaders):*
  »Oracle«, »IBM«, »Novell«, »Sun Microsystems«, »CA«, »Courion«
- Izzivalci *(ang. challengers):*
  »Hitachi ID Systems«, »Siemens«, »BMC Software«, »Beta Systems«, »Avatier«, »Microsoft«
- Nišni proizvajalci *(ang. niche players):*
  »Omada«, »Quest Software« , »Evidian«, »Ilex«, »SAP«
- Vizionarji *(ang. visionaries):*
  »Sentillion«, »Volcker Informatik«, »Fischer International«



Slika 4.3: Gartnerjev magični kvadrant sistemov za oskrbovanje uporabnikov, 09/2009[10]

4.4.1. Kratek pregled vodilnih proizvajalcev sistemov za oskrbovanje uporabnikov

V nadaljevanju sledi kratek pregled vodilnih proizvajalcev na trgu sistemov za oskrbovanje uporabnikov na podlagi Gartnerjevega poročila[**10**]. K temu pregledu sem dodal tudi rešitev podjetja Microsoft, ki sicer ne spada med vodilne izdelke na trgu, je pa podjetje vseeno zelo pomemben igralec na celotnem IAM trg. Poglavitni razlog za vključitev v kratek pregled je pa ta, da bo njihov izdelek predmet primerjave v nadaljevanju tega diplomskega dela. Microsoft sem izbral na podlagi dejstva, da podjetje s svojim imeniški sistemom Active Directory na trgu imeniških storitev zaseda vodilno vlogo [**9**] in me zanima zakaj na področju oskrbovanja uporabnikov zaostaja za vodilno konkurenco.

4.4.1.1. Oracle

Oracle IAM Suite in Oracle Identity Manager v.9.1.0.2 (Januar 2009)

- Sodeč po zadnji raziskavi je Oracle vodilni proizvajalec na trgu sistemov za oskrbovanje uporabnikov. Še naprej dosledno izvajajo svojo vizijo integriranih in razširljivih izdelkov, ki jih ponujajo tudi kot celovit sistem za upravljanje identitet - »IAM Suite«.
- Oracle Identity Manager platforma lahko deluje na dveh različnih podatkovnih bazah, sedmih različnih operacijskih sistemih ter štirih različnih aplikacijskih strežnikih.

- Oracle še naprej izkazuje močno rast strank s pomočjo prevzemov, ter s svojo širitvijo prodajne mreže. Prevzem podjetja Sun Microsystems, ki se je zgodil pred kratkim naj bi bil končan do poletja 2010.
- Oracle je kot vodilni izdelovalec podatkovnih baz uspel prodreti v številnih državah tudi do javnega sektorja.
- Agresiven marketinški pristop in tržna strategija se kažeta v pospešeni prodaji in stopnji rasti strank, ki je večkratnik stopnje rasti celotnega trga sistemov za oskrbovanje uporabnikov.
- Oraclov interes je bil, da svojo mrežo globalnih partnerstev ustrezno usposobi za uvajanje najboljših praks pri implementaciji in vzdrževanju IAM izdelkov. Rezultat tega pristopa je, da so njegovi partnerji - sistemski integratorji postali veliko bolj izkušeni. Med njimi so svetovno znane revizijske hiše, ko so Deloitte, Accenture, KPMG, PricewaterhouseCoopers in Wipro.
- Kupci njihovih izdelkov cenijo dostopnost Oraclovih razvojnih skupin, ki so dovzetne za njihove predloge, predvsem pri izboljšavah izdelka in nedavno posodobljeno knjižnico konektorjev.

4.4.1.2. IBM Tivoli

IBM Tivoli Identity Manager (ITIM) v.5.1 (Junij 2009), ITIM za z/OS v.5.0 (Avgust 2008) in ITIM Express v.4.6 (Marec 2006)

- IBM Tivoli je globalni igralec v več segmentih IT upravljanja, vključno z upravljanjem storitev, in se je v zadnjih desetih letih uspešno razširil tudi na področje IAM trga.
- Tudi IBM širi svoj IAM portfelj s prevzemi podjetij, ki dopolnjujejo njegovo ponudbo.
- IBM Tivoli verzije 5.1 je izboljšal svojo učinkovitost na področju enostavnejše uporabe in boljše integracije s komponentami iz njegove zbirke celovitih rešitev za upravljanje identitet.
- Tehnologije oskrbovanja uporabnikov in potrjevanja delovnih tokov so relativno popolne in nudijo obsežno zbirko konektorjev.
- Nudijo tudi razvojni komplet, ki omogoča enostavnejši razvoj prilagojenih konektorjev za sisteme, ki še niso podprti. Upravljanje z gesli in delegirana administracija sta prav tako zelo konkurenčni.

4.4.1.3. Sun Microsystems

Sun Identity Manager v.8.1 (Junij 2009) — Sun Role Manager v.4.1

- Kljub negotovosti glede pridobivanja novih strank zaradi prevzema s strani Oracla je Sun še vedno podjetje iz vodilnega kvadranta za leto 2009.
- To jim uspeva s strokovnimi znanji in izkušnjami ter različnimi oblikami partnerstev, ki vključujejo zelo izkušene svetovalce in sistemske integratorje.

- Sun je vodilni med proizvajalci sistemov, ki ponujajo odprtokodne rešitve, tudi njihov sistem za oskrbovanje uporabnikov sledi temu zgledu licenciranja.
- Sedemdeset odstotkov Sunovih sistemov za oskrbovanje uporabnikov je nameščenih pri strankah, ki imajo 50.000 ali več uporabnikov, s čimer je Sun eden izmed najbolj izkušenih proizvajalcev pri zagotavljanju teh rešitev za velika podjetja.

4.4.1.4. Novell

Novell Identity Manager Roles Based Provisioning Module v.3.6.1, Designer for Novell Identity Manager v.3.6.1, Novell Sentinel v.6.1, Novell Identity Audit v.1.0 in Novell Identity Assurance Solution v.3.0

- Novell še izboljšuje svojo pozicijo v vodilnem kvadrantu, čeprav počasneje, kot je bil ta napredek v letu 2008.
- To jim uspeva s poudarkom na partnerstvih, prodaji in trženju izdelkov
- Njihovi IAM izdelki so zelo homogeni, saj so organsko rasli znotraj podjetja in skoraj brez prevzemov. Tako je portfelj njihovih izdelkov veliko bolj integriran v celovit sistem za upravljanje identitet, kot je to v navadi pri konkurentih iz vodilnega kvadranta.
- Novell stavi na strategijo manjših, regionalnih partnerstev in se hkrati povezuje z nekaterimi globalnimi korporacijami, kot so Atos Origin, Deloitte, Wipro ter HP in SAP.
- Novell je aktivni udeleženec v odprtokodnem identitetnem ogrodju, ki zajema tudi oskrbovanje uporabnikov, preko svojega članstva v projektu Eclipse Higgins.
- Novell je dejaven pri mednarodnih standardih z vlogo, ki jo ima na področju Linuxa, varnosti ter identitet. Novell Identity Manager podpira tudi SPML.

4.4.1.5. CA

CA Identity Manager Release 12 (Junij 2008), CA Role & Compliance Manager Release 12

- CA je izdelovalec, ki je po Gartnerjevih merilih v letu 2009 najbolj napredoval v vodilnem kvadrantu.
- CA Identity Manager temelji na izdelku IdentityMinder (iz leta 2002) in eTrust Admin (iz leta 2000), in ima zato zelo dolgo dediščino na trgu IAM sistemov.
- Tudi CA je svoj portfelj IAM razvijal s prevzemi in tako zelo uspešno razširili zmogljivosti svojih izdelkov
- CA igra aktivno vlogo pri mednarodnih identitetnih/varnostnih standardih, ki se tičejo oskrbovanja uporabnikov. Podprti so tehnični standardi (kot recimo SPML) in standardi upravljanja storitev (kot je ITIL).

- Večji partnerji in sistemski integratorji s katerimi se povezujejo vključujejo podjetja, kot so Deloitte, Capgemini in PricewaterhouseCoopers, Logic Trends, Rolta in TCS.

4.4.1.6. Courion

Courion Access Assurance Suite (AccountCourier) v.8.0 (April 2008)

- Courion ohranja mesto v vodilnem kvadrantu in dosega določen napredek predvsem zaradi izboljšane tržne strategije, tehničnih inovacij ter razširitvi portfelja na področju IAM obveščanja (analiza, revizija, poročanje).
- Courion je eden redkih proizvajalcev, ki strankam ponuja fiksno ceno pri implementaciji svojega sistema. To zahteva strogo načrtovanje pred samo implementacijo sistema in zaupanje stranke v uspeh.
- Nedavno so integrirali v sistem tudi upravljanje življenjskega cikla vloge uporabnika.
- Sistem je rasel organsko znotraj podjetja in brez prevzemov, kar omogoča enostavnejšo integracijo v mnogih primerih uporabe.
- Kljub temu, da je 70% njihovih strank iz segmenta manjših podjetij, so razširili svoj domet in začeli prodajati razširljive sisteme za večje stranke.
- Kupci cenijo njihovo preprosto in kompaktno arhitekturo, hitro uvajanje, osredotočanje na zahteve uporabnikov, ter fleksibilnost pri konfiguraciji in prilagajanju sistema potrebam stranke.

4.4.1.7. Microsoftov pristop k oskrbovanju uporabnikov

Microsoft Identity Lifecycle Manager (ILM) (Maj 2007), Feature Pack 1 (Oktober 2007) z možnostjo upravljanja certifikatov

- Microsoft se s svojim sistemom uvršča v kvadrant izzivalcev.
- Microsoftov Active Directory in identitetni repozitoriji, ki temeljijo na AD so dandanes skoraj povsod navzoči. Zaradi tega se večina podjetij, ki iščejo alternativo vodilnim proizvajalcem na trgu IAM rešitev, obrne na Microsoft.
- Microsoft pri stroških licenciranja in implementacije ostaja najcenejši med ponudniki. Nudijo izdelek, ki zadovolji osnovne potrebe pri oskrbovanju uporabnikov za 50% do 65% cene, ki jo nudijo vodilni konkurenti.
- Strankam je všeč bogata in tesna povezanost ILMja z Active Directory-em in ravnotežje med funkcionalnostjo ter razširljivostjo izdelka v primerjavi s kompleksnostjo ter stroški.
- Microsoft je že za leto 2008 napovedoval splavitev izdelka ILM 2, ki se bo preimenoval v Forefront Identity Manager. Nova, izboljšana verzija izdelka bi naj po napovedih Microsoftovih inženirjev končno resneje konkurirala vodilnim izdelkom na trgu IDMS.

Poglavje 5:

OPIS: ORACLE IDENTITY MANAGER IN MICROSOFT IDENTITY LIFECYCLE MANAGER

Poglavje pet nudi kratko predstavitev dveh sistemov za oskrbovanje uporabnikov, ki ju bom v nadaljevanju tega dela preizkusil tudi v praksi: »Oracle Identity Manager« in »Microsoft Identity Lifecycle Manager«. Poglavje je strukturirano na enovit način, zato si predstavitev obeh sistemov sledi po naslednjem zaporedju: evolucija izdelka, lastnosti, arhitektura sistema ter podprta okolja. Evolucija izdelka nudi vpogled v razvoj in dinamiko razvoja posameznega izdelka. Veliko izdelovalcev je namreč linijo izdelkov za upravljanje identitet dograjevalo z nakupi in prevzemi konkurenčnih podjetij, temu primerno so se menjavala blagovne znamke izdelkov in večala zmeda med zainteresirano javnostjo. Opisu lastnosti oziroma funkcionalnosti sistemov sledi še arhitektura sistema. Slednja nudi vpogled v najpomembnejše komponente oziroma module. Predstavitev zaokrožim s pregledom podprtih okolij in vgrajenih adapterjev oziroma konektorjev, ki jih nudi posamezen sistem za povezovanje z oddaljenimi viri.

5.1. Oracle Identity Manager

Oracle Identity Manager *(krat. OIM)* je zelo prožen in prilagodljiv sistem za upravljanje identitet. Upravlja s pravicami in dostopi do informacijskih virov organizacije. Pomaga odgovoriti na kritična vprašanja o skladnosti: »Kdo ima dostop do česa, kdaj, kako in zakaj?«[**22**]

5.1.1. Evolucija izdelka

Podjetje Oracle je svoj izdelek za upravljanje identitet začelo razvijati s prevzemi manjših podjetij, ki so izdelovala takšne sisteme. V začetku 2005 so prevzeli podjetje »Oblix«, ki je razvilo »COREid Provisioning« sistem. Maja 2005 je Oracle na trg splavil izdelek pod svojo blagovno znamko, kot »Oracle COREid Provisioning«. Izdelek je bil na trgu vsega nekaj mesecev, saj so konec istega leta prevzeli še »Xellerate Identity Provisioning« proizvajalca »Thor«. Sistem se je od takrat naprej prodajal pod imenom »Oracle Xellerate Identity Provisioning«. Oracle je sčasoma izdelek popolnoma integriral v svoj portfelj upravljanja identitet in se danes imenuje »Oracle Identity Manager«, trenutna verzija izdelka je 9.1.0.1. Izdelek je na voljo kot delni sistem ali pa v paketu za celovito upravljanje identitet, pod imenom »Identity management«, ki spada v linijo izdelkov »Oracle Fusion Middleware«. [**2**,**18**,**19**]

5.1.2. Lastnosti

Sklicujoč se na [**22**], bom naštel nekatere ključne funkcionalnosti, ki jih nudi OIM.

Samostrežna in delegirana administracija:

- Preko samopostrežnih vmesnikov lahko končni uporabnik sam ureja svoj uporabniški profil in tako razbremenjuje administratorje.
- Zahtevo za dostop do določenega informacijskega vira je prav tako mogoče oddati preko samopostrežnih vmesnikov. Vodjem skupin, oddelkov, enot, itn. pa isti vmesniki omogočajo odobritev ali zavrnitev oddanih zahtevkov.
- Delegirana administracija omogoča pooblastitev uporabnikov in/ali skupin za upravljanje določenih administracijskih nalog.

Delovni tokovi in varnostne politike:

- Omogočajo avtomatizirano oskrbovanje identitet z dovoljenji za dostop do virov na podlagi zelo podrobno nastavljenih pravic.
- Omogočajo ločeno delovanje delovnih tokov, namenjenih oskrbovanju identitet in potrjevanju dovolilnic.

- Nudijo »deprovisioning« - zaposlenim, ki zapustijo organizacijo, nemudoma preprečijo dostop do informacijskih virov.
- Integriteta transkacij skupaj z varnostnimi politikami omogoča skladnost podatkov (možna razveljavitev transakcij in vzpostavitev prejšnjega stanja)

Upravljanje gesel:

- Samopostrežno upravljanje gesel omogoča, da si uporabnik sam ponastavi geslo preko samopostrežnih vmesnikov v primeru, da ga je pozabil.
- Napredne varnostne politike upravljanja z gesli končnega uporabnika silijo k tvorjenju kompleksnih gesel glede na njegove pravice dostopa do virov. Večji privilegiji zahtevajo kompleksnejša gesla in obratno.
- Omogoča sinhronizacijo gesel med oddaljenimi viri za večino vgrajenih adapterjev.

Revizija sistema in skladnost s predpisi:

- Usklajevanje identitet z oddaljenimi sistemi deluje tudi v primeru, ko so bile spremembe narejene na oddaljenih sistemih in ne preko OIM vmesnika.
- Odkrivanje in nadzor slepih *(ang. rogue)* in osirotelih *(ang. orphan)* računov. Slep uporabniški račun je tak, ki je bil ustvarjen izven nadzora sistema za oskrbovanje uporabnikov. Osirotel račun pa je račun brez veljavnega uporabnika. Oboji predstavljajo resno varnostno grožnjo organizacijam.
- Izčrpno poročanje in revizija omogočata preverjanje skladnosti in spremljanje zgodovine uporabniških identitet.

5.1.3. Arhitektura sistema

Oracle Idenity Manager je zgrajen na modularni arhitekturi, ki je hkrati odprta in razširljiva. Vsak izmed modulov ima ključno vlogo pri splošni funkcionalnosti sistema. »Slika 5.1« prikazuje komponente oziroma module tega sistema.

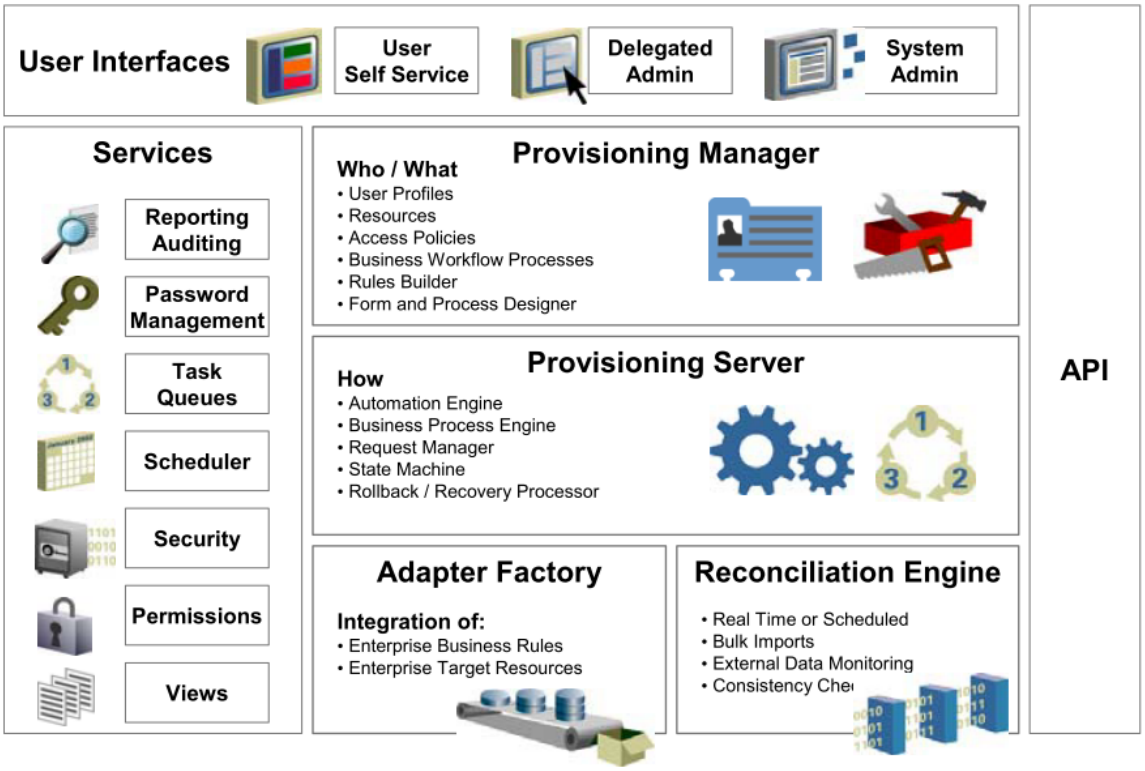
Uporabniški vmesniki OIM opredeljujejo in upravljajo celotno okolje sistema za oskrbovanje uporabnikov. OIM ponuja dva funkcionalno bogata uporabniška vmesnika za zadovoljitev administratorskih kakor tudi uporabniških zahtev:

»Design Console«:

Je zmogljiva, na programskem jeziku Java temelječa konzola za razvijalce in sistemske administratorje.

»Administration and User Console«:

Je spletni upravljavski vmesnik za administratorje identitet in končne uporabnike.



Slika 5.1: Komponente OIM [22]

Sledi pregled nekaterih ključnih funkcionalnosti sistema OIM, kot jih prikazuje »Slika 5.1«:

»ProvisionManager«:

ProvisionManager *(slov. Upravljavec oskrbovanja)* je modul, v katerem se sestavljajo in spreminjajo transakcije. Skrbi za politike tipa »kdo« in »kaj« oskrbovanja uporabnikov. Preko njega se nastavljajo uporabniški profili, dostopne politike, viri, poslovna pravila in procesi ter delovni tokovi.

»ProvisionServer«:

Je izvajalski pogon, ki izvršuje procese transakcij oskrbovanja uporabnikov, ki so opredeljeni s pomočjo vmesnika »Design Console« in vzdrževani s strani »ProvisionManager-ja«. Več o tem je obrazloženo v »poglavju 3.4.1.1.a.«

»Adapter Factory«:

»Adapter Factory« gradi in vzdržuje integracije med OIM in oddaljenimi sistem ter aplikacijami, ki jih le-ta upravlja. Odpravlja potrebo po vgradnem kodiranju integracije s temi sistemi. S preslikavo procesa oskrbovanja uporabnikov iz OIM neposredno na ciljno konfiguracijo oddaljene aplikacije ali sistema, omogoča administratorjem delo na višji ravni abstrakcije. Ko je preslikava vzpostavljena, bo »Factory Adapter« ustvaril vso potrebno kodo za integracijo z oddaljenim sistemom ali aplikacijo. Spremembe in razširitve adapterjev se izvajajo z delom na preslikavi in ne s kodo.

»Reconciliation Engine«:

Modul »Reconciliation Engine« *(slov. pogon za usklajevanje identitet)* skrbi za skladnost identitet z oddaljenimi sistemi. Usklajuje in sinhronizira identitete, ki so bile spremenjene ali ustvarjene neposredno na oddaljenih virih in ne preko OIM vmesnika. Za zagotavljanje skladnosti sinhronizira tudi poslovna pravila, ki so izven nadzora sistema za oskrbovanje uporabnikov.

5.1.4. Podprta okolja

Osnovna namestitev OIM je sestavljena iz:

- Relacijske podatkovne baze, ki služi kot repozitorij
- Aplikacijskega strežnika
- OIM namestitve, ki teče na aplikacijskem strežniku
- vmesnika »Design Console«, ki teče v »Java« okolju
- vmesnika »Administation and User Console«, ki teče v spletnem brskalniku

Namestitvene zahteve in podprta okolja	
Aplikacijski strežniki:	JBoss Application Server BEA WebLogic Server IBM WebSphere Application Server Oracle Application Server
Operacijski sistemi:	Microsoft Windows Linux Solaris
Relacijske podatkovne baze:	Microsoft SQL Server Oracle Database

Tabela 5.1: Namestitvene zahteve in podprta okolja za Oracle Identity Manager 9.1.0.1 [21]

»Tabela 5.2« nudi pregled že vgrajenih adapterjev v OIM, ki podpirajo povezavo z oddaljenimi sistemi.

Vgrajeni adapterji	
BMC:	BMC Remedy User Management BMC Remedy Ticket Management
Computer Associates:	CA ACF2 Advanced CA Top Secret Advanced
IBM:	IBM RACF Standard IBM RACF Advanced IBM OS/400 Advanced IBM Lotus Notes and Domino
Microsoft:	Microsoft Active Directory User Management

	Microsoft Active Directory Password Synchronization Microsoft Exchange Microsoft Windows
Novell:	Novell eDirectory Novell GroupWise
Oracle:	JD Edwards EnterpriseOne User Management Oracle E-Business Employee Reconciliation Oracle E-Business User Management Oracle Internet Directory Oracle Retail Warehouse Management System PeopleSoft Employee Reconciliation PeopleSoft User Management Siebel User Management
Relacijske podatkovne baze:	*Database User Management:* IBM DB2, Microsoft SQL Server, Oracle Database, Sybase DB) *Database Application Tables:* IBM DB2 9.x, Microsoft SQL Server 2005, 2008, Oracle Database 10g, 11g, Sybase Adaptive Server Enterprise 15.0.2
RSA	RSA Authentication Manager RSA ClearTrust
SAP:	SAP CUA SAP Employee Reconciliation SAP Enterprise Portal SAP User Management
Sun:	Sun Java System Directory
UNIX:	UNIX SSH UNIX Telnet

Tabela 5.2: Pregled vgrajenih adapterjev/konektorjev za Oracle Identity Manager 9.1.0.1 [*20****]***

5.2. Microsoft Identity Lifecycle Manager

»Microsoft Identity Lifecycle Manager 2007 Feature Pack 1« *(krat. ILM ali ILM 2007 FP1)* je blagovna znamka podjetja Microsoft za linijo izdelkov, ki spadajo v segment upravljanja identitet in dostopov. ILM 2007 združuje meta imenik, upravljanje s certifikati in oskrbovanje uporabnikov na različnih sistemih v enem paketu.

5.2.1. Evolucija izdelka

Trenutna verzija izdelka je bila splavljena na trg že leta 2007, in sicer z združitvijo izdelkov »Microsoft Identity Integration Server 2003« *(krat. MIIS)* in »Microsoft Certificate Lifecycle Manager« *(krat.*

CLM). Zasnova izdelka se ni spremenila vse od izdaje MIIS 2003. Iz tehnološkega vidika je bil napredek z dodanim CLM-jem k paketu le neznaten.[**33**]

Gledano iz tehnološke perspektive je MIIS 2003 v bistvu meta imenik (razlaga v »poglavju 3.2.1.4«) s funkcijami za oskrbovanje uporabnikov. Izvirna različica Microsoftovega meta imenika je bila v preteklosti znana kot Microsoft Metadirectory Services *(krat. MMS)*. Ta različica je bila sicer učinkovita, vendar zelo kompleksna za upravljanje. Veliko komponent je bilo potrebno ročno nastavljati s skriptnim jezikom, da je imenik sploh pravilno deloval - zelo neprijazno do uporabnika. Tudi podpora izdelkom drugih proizvajalcev, je bila minimalna. S splavitvijo verzije 3.0 se je spremenila blagovna znamka in izdelek se je preimenoval v MIIS 2003. MIIS je bil popolnoma prenovljen produkt, veliko prijaznejši do uporabnikov. Sočasno z izdajo strežniškega operacijskega sistema se je podjetje ponovno odločilo za preimenovanje blagovne znamke, ki se danes imenuje »Identity Lifecycle Manager 2007«. ILM 2007 poseduje več funkcionalnosti, kot predhodniki, le-te bodo predstavljene v nadaljevanju. Z vgrajenimi upravljavskimi agenti omogoča sinhronizacijo z večjim številom različnih imenikov, podrobnosti o agentih so navedene v »Tabeli 5.4«.[**17**]

Oktobra 2007 je Microsoft izdal še »ILM 2007 Feature Pack 1« edicijo, ki je do trenutka pisanja tega diplomskega dela tudi najnovejša različica sistema in bo predmet primerjave v nadaljevanju. Dodani so bili agenti za podporo »čistim Exchange 2007 okoljem«, ter nekatere druge razširitve za digitalna potrdila, pametne kartice ter podpora operacijskemu sistemu Vista.

5.2.2. Lastnosti

Sklicujoč se na [**16**], bom naštel nekatere ključne funkcionalnosti, ki jih ima sistem. ILM 2007 FP1 je oblikovan za poenostavitev in avtomatizacijo nekaterih, finančno najdražjih vidikov upravljanja življenjskega cikla. ILM 2007 FP1 omogoča organizacijam:

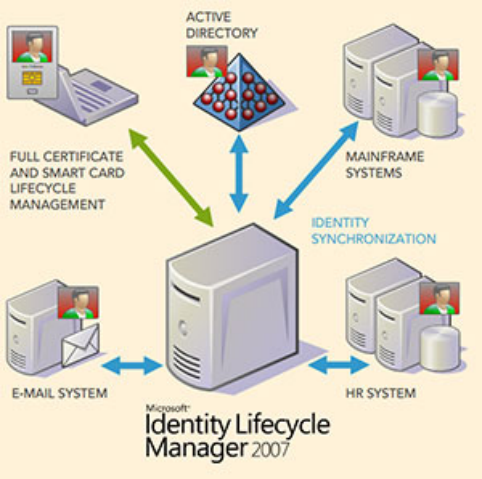
Sinhronizacija informacij o identitetah:

- Omogoča enoten pogled uporabnikov čez vse sisteme in samodejno skrbi za konsistenco informacij o identitetah.
- Organizacije, ki imajo veliko različnih imenikov in drugih zbirk podatkov, kot so recimo podatki v repozitorijih kadrovskih služb, »mainframe« sistemih in ostalih bazah podatkov, lahko uporabijo ILM 2007 FP1 za sinhronizacijo uporabniških računov ter atributov v vseh teh sistemih, vključno s sinhronizacijo gesel.

Oskrbovanje uporabnikov:

- Avtomatizira proces kreiranja in ukinjanja uporabnikov, poenostavlja skladnost skozi avtomatizacijo oskrbovanja identitet, skrbi za skladnost poverilnic med sistemi.

- V mnogih organizacijah, se informacije o novih zaposlenih najprej vnesejo v kadrovsko bazo podatkov. Potem IT oddelek ustvarja uporabniške račune, poštne predale, in druge uporabniške podatke v različnih sistemih ter podatkovnih zbirkah.
- ILM 2007 FP1 omogoča samodejno ustvarjanje uporabniških računov, poštnih predalov, in drugih uporabniških podatkov v ciljnih sistemih v realnem času. Tako lahko novi zaposleni začnejo z delom takoj, in ne šele čez nekaj dni po vstopu v organizacijo.
- ILM omogoča organizacijam tudi to, da zaposlenim, ki zapustijo organizacijo, nemudoma preprečijo dostop do virov.



Slika 5.2: Lastnosti ILM 2007 FP1

Upravljanje s certifikati in pametnimi karticami:

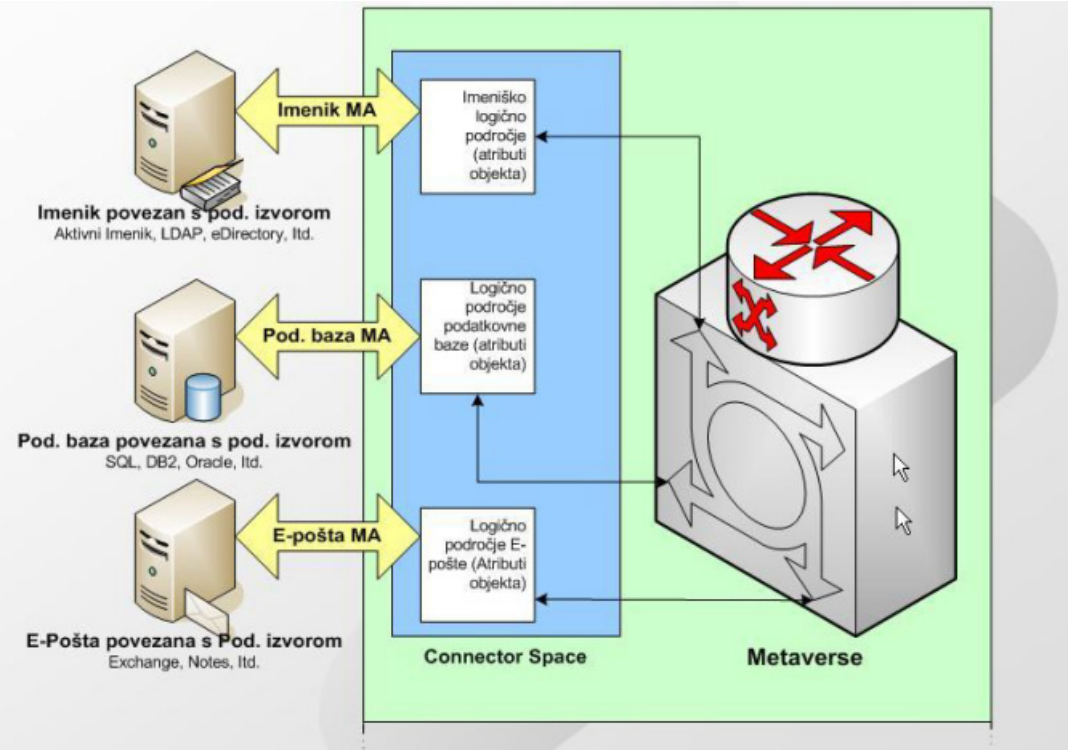
- Prinaša enotno točka skrbništva za digitalna potrdila in pametne kartice.
- Avtomatizira delovni tok izdajanja in odvzemanja certifikatov, poenostavi izdajanje pametnih kartic, integracija z obstoječo infrastrukturo.

5.2.3. Arhitektura sistema

ILM 2007 FP1 ima dva bistvena sestavna dela. Prvi sestavni del vključuje meta imenik in funkcionalnosti oskrbovanja uporabnikov, drugi bistveni sestavni del pa skrbi za upravljanje s certifikati in pametnimi karticami.[**16**] V nadaljevanju se bom osredotočil na prvega, ker bo le-ta tudi predmet primerjave. Njegovo arhitekturo prikazuje »Slika 5.3«.

Za lažje razumevanje tehnologije sistema bom najprej razložil nekatere najpogosteje uporabljene termine, specifične za ILM. Nekateri od njih so prikazani na »Sliki 5.3«. Pri tem se opiram na vire [**1**,**17**].

- **Management Agent *(krat. MA)*** Je komponenta ILM, ki poveže oddaljen podatkovni izvor z ILM in izvede operacije izvoza in uvoza. (Več o konektorjih je razloženo v »poglavju 3.4.1.1.d«)
- **Connected Directory *(krat. CD)*** Je ime oddaljenega podatkovnega izvora. Uporablja se neodvisno od tega, ali je izvor podatkovna baza ali imeniški strežnik.
- **Connector Space *(krat. CS)*** Področje ILM repozitorija, ki se uporablja za shranjevanje kopij podatkov iz različnih CD-jev, na katere smo povezani, v ILM imeniku. Tehnično gledano pa je to v bistvu samo tabela shranjena v SQL Serverju.
- **Metaverse *(krat. MV)*** Je v bistvu meta imenik (Več o tem »poglavje 3.2.1.4.d«). Tu se informacije o identitetah iz različnih CS-jev agregirajo v eno identiteto.
- **MA extension** Določeno kodiranje, ki razširi operacije MA, z namenom, da bi se izvedlo več kompleksne podatkovne manipulacije, kot jo je na razpolago skozi grafični vmesnik.
- **MV extension** Določeno kodiranje, ki razširi operacije MV, da zagotovi osnovne storitve.



Slika 5.3: komponente ILM 2007 FP1[1]

5.2.4. Podprta okolja

Osnovna namestitev ILM je sestavljena iz:

- Relacijske podatkovne baze
- ILM namestitve, ki teče na strežniškem operacijskem sistemu

Namestitvene zahteve in podprta okolja	
Operacijski sistemi:	Microsoft Windows Server 2003 / 2008
Relacijske podatkovne baze:	Microsoft SQL Server 2000 SP4 / 2005 SP2

Tabela 5.3: Namestitvene zahteve in podprta okolja za Microsoft ILM 2007 FP1

Za povezavo z oddaljenimi podatkovnimi izvori se uporabljajo adapterji. »Tabela 5.4« nudi pregled že vgrajenih adapterjev v ILM 2007 FP1 za povezavo z oddaljenimi podatkovnimi izvori, oziroma imeniki.

Vgrajeni adapterji	
Computer Associates:	Computer Associates eTrust ACF2 in Top Secret
IBM:	IBM Tivoli Directory Server do verzije 6.2 IBM Lotus Notes 4.6/5.0/6.x IBM Resource Access Control Facility IBM iSeries security (IBM OS/400)
Microsoft:	Windows NT 4.0 Windows 2000/2003/2003 R2/2008 Active Directory Active Directory Lightweight Directory Services (AD LDS) and legacy Active Directory in Application Mode (ADAM) Microsoft Exchange 2007, 2003, 2000, in 5.5
Novell:	Novell NDS in eDirectory 8.x
Ostalo:	XML- in DSML-osnovani sistemi Datotečni formati (Attribute Value Pairs, CSV, Fixed Width, Delimited) LDAP Interchange Format (LDIF) datoteke
Relacijske podatkovne baze:	IBM DB2 Microsoft SQL Server 7.x/2000/2005/2008 Oracle 8i/9i/10g
SAP:	SAP 4.7/5.0
Sun:	Sun Directory Server 4.x/5.x/6.x

Tabela 5.4: Pregled vgrajenih adapterjev/konektorjev za ILM 2007 FP1[16,17]

Poglavje 6:

OSKRBOVANJE UPORABNIKOV V PRAKSI: OIM V PRIMERJAVI Z ILM

V pričujočem poglavju bom na podlagi praktične implementacije scenarija problemske domene primerjal dva sistema za oskrbovanje uporabnikov.

Skušal bom ugotoviti kako se Microsoftov izdelek v praksi obnese v primerjavi z Oraclovim. Primerjal bom torej sistema »Oracle Identity Manager 9.1.0.1« ter »Microsoft Identity Lifecycle Manager 2007 FP1«. Izbor slednjih je nastal iz zahteve, da bom preizkusil vodilni izdelek na trgu z enim izmed izzivalcev. Ob dejstvu, da podjetje Microsoft s svojim imeniški sistemom Active Directory na trgu imeniških storitev zaseda vodilno vlogo [**9**], sem bil toliko bolj presenečen, da na področju oskrbovanja uporabnikov, glede na dognanja iz pregleda sistemov v »poglavju 4.4.«, zaostaja za konkurenco.

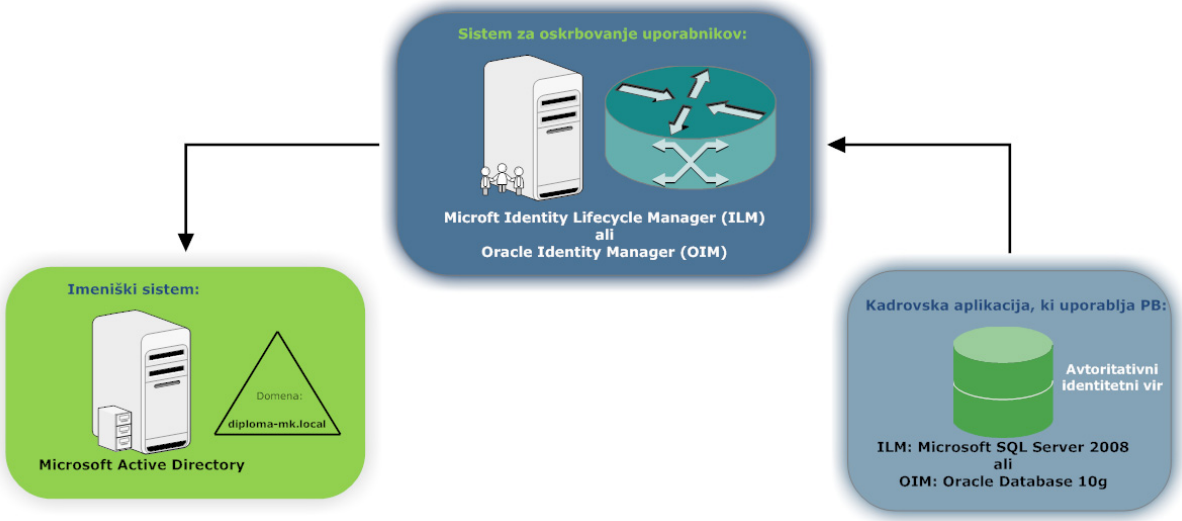
Za postavitev testnega okolja sem uporabil navidezni stroj »VMware Workstation 6.5.3«. Testiranje je potekalo na operacijskem sistemu »Windows Server 2008 sp2«. Kratka predstavitev obeh sistemov, ki ju bom preizkusil v nadaljevanju pa se nahaja v »poglavju 5« tega dela.

6.1. Problemska domena

Za primerjavo sistemov sem si izbral tipični scenarij, ki avtomatizira administratorska opravila, kadar se v organizaciji zaposli novi sodelavec oziroma ko zaposleni organizacijo zapusti. V testnem scenariju bom prikazal tipične operacije, ki so potrebne pri dodeljevanju in odvzemanju pravic za dostop do

informacijskih virov *(ang. provisioning / deprovisioning)* na obeh sistemih za oskrbovanje uporabnikov.

V mnogih organizacijah se informacije o novem zaposlenem najprej vnesejo v kadrovski informacijski sistem. Zato sem predpostavil, da ima organizacija kadrovsko aplikacijo, ki za svoje delovanje uporablja tabelo v podatkovni bazi. Potem, ko je nov sodelavec shranjen v podatkovni bazi, mora sistem za oskrbovanje uporabnikov novemu zaposlenemu ustvariti še uporabniški račun v imeniškem sistemu Microsoft Active Directory. Prav slednji je najbolj razširjeni imeniški sistem v organizacijah. Za potrebe testiranja scenarija problemske domene sem v Microsoftovem AD ustvaril korensko AD domeno: *diploma-mk.local*. Za lažje razumevanje pravkar zapisanega, prikazuje »Slika 6.1« celotno arhitekturo scenarija problemske domene.



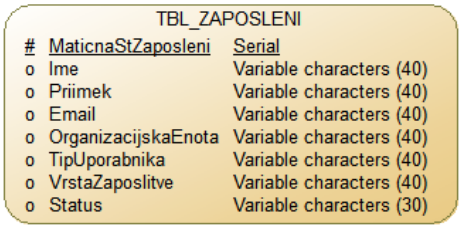
Slika 6.1: Arhitektura scenarija problemske domene

Poenostavljeno povedano: na vsakem izmed obravnavanih sistemov za oskrbovanje uporabnikov bom implementiral scenarij problemske domene. V obeh testiranih sistemih bom skušal avtomatizirati sinhronizacijo uporabniških identitet iz tabele podatkovne baze v Microsoftov AD. Kreiranje ter brisanje uporabniških računov v AD domeni se bo izvajalo na podlagi zapisov, ki so shranjeni o vsakem zaposlenem v avtoritativnem identitetnem viru, torej tabeli, ki je shranjena v podatkovni bazi. Na koncu bom podal svoje ugotovitve in izkušnje, ki sem jih pridobil z obema sistemoma.

Za potrebe scenarija problemske domene sem pri shranjevanju avtoritativnih podatkov vedno izbral podatkovno bazo, ki jo obravnavani sistem uporablja kot repozitorij za shranjevanje metapodatkov. V scenariju z OIM je bila to podatkovna baza »Oracle Database 10g« in za ILM podatkovna baza »Microsoft SQL Server 2008«.

Konceptualni model tabele v kateri so shranjeni podatki o zaposlenih prikazuje »Slika 6.2« in predstavlja močno poenostavitev konceptualnih modelov realnih kadrovskih sistemov. Poenostavitev sem si dovolil iz razloga, ker se v praksi realne-kompleksnejše sisteme, ki uporabljajo mnogo več tabel, pred povezavo s sistemom za oskrbovanje uporabnikov vedno lahko prevede na podobno tabelo oziroma pogled *(ang. view)*. Pogled je rezultat ene ali več operacij nad osnovnimi relacijami z namenom pridobitve nove relacije. Pogledi, ki jih je smotrno predhodno kreirati v podatkovni bazi predstavljajo podmnožico identitetnih atributov realnega kadrovskega sistema, ki jih potrebuje sistem IDM za svoje delovanje, oziroma v mojem primeru za sinhronizacijo identitet. Delo s takšno tabelo oziroma pogledom je nato v samem sistemu za oskrbovanje uporabnikov pri definiranju preslikav atributov mnogo enostavnejše.

Tabela, ki jo prikazuje »Slika 6.2« predstavlja v mojem testnem scenariju problemske domene avtoritativni vir podatkov.



Slika 6.2: Konceptualni model: Tabela s podatki o zaposlenih

To pomeni, da se informacije o novih zaposlenih najprej shranijo v to tabelo. Tudi kasnejše spremembe informacij o zaposlenih se v podrejenem informacijskem viru (Active Directory) in sistemu za oskrbovanje uporabnikov, izvršujejo na podlagi te tabele. Za nadaljnjo obravnavo je pomemben atribut Status, ki ima lahko eno izmed naslednjih vrednosti: Aktiven *(ang. Active)* ali Izbrisan *(ang. Deleted)*. Ti vrednosti določata kakšen je trenuten status zaposlenega v organizaciji. V kolikor je le-ta še vedno zaposlen v organizaciji ima status »Active«, v kolikor je organizacijo že zapustil dobi status »Deleted«.

6.2. Oracle Identity Manager 9.1.0.1

6.2.1. Namestitev

Namestitev OIM je lahko zelo zahtevno opravilo, saj je možna vrsta kombinacij različnih namestitev, kot je razvidno iz »poglavja 5.1.4«, podprta je celo namestitev v gruče. Iz tega razloga sem za potrebe

diplomskega dela skušal izbrati čim bolj preprosto kombinacijo. Namestitev OIM je bil za moj testni scenarij problemske domene sestavljena iz relacijske podatkovne baze ter aplikacijskega strežnika:

- *Relacijska podatkovna baza:* »Oracle Database 10g (10.2.0.3)«
- *Aplikacijski strežnik:* »Oracle WebLogic Server 10.3« (včasih BEA WebLogic Server)

Pred namestitvijo odjemalca OIM je potrebno konfigurirati še podatkovno bazo, ki bo služila kot repozitorij, kar se običajno naredi s prilagoditvijo in zagonom skripte »prepare_xl_db.bat«. Podrobnosti o tem, ter nasploh o različnih kombinacijah namestitev si lahko zainteresiran bralec prebere tukaj [**21**]. Nato sledi namestitev strežnika »Oracle Identity Manager 9.1.0.1« na aplikacijskem strežniku. Ko je postopek končan, namestimo še javanskega odjemalca »OIM Design Console«. Po namestitvi strežnik zaženemo preko skripte »xlStartServer.bat«, ki se nahaja v `OIM_HOME\xellerate\bin\` direktoriju. Aplikacijskega strežnika ni treba predhodno zaganjati, saj za vse poskrbi prej omenjena skripta. Po zagonu OIM strežnika sta na voljo oba administracijska vmesnika, kratek opis njunih funkcionalnosti predstavljam v nadaljevanju.

6.2.2. Administracijska vmesnika

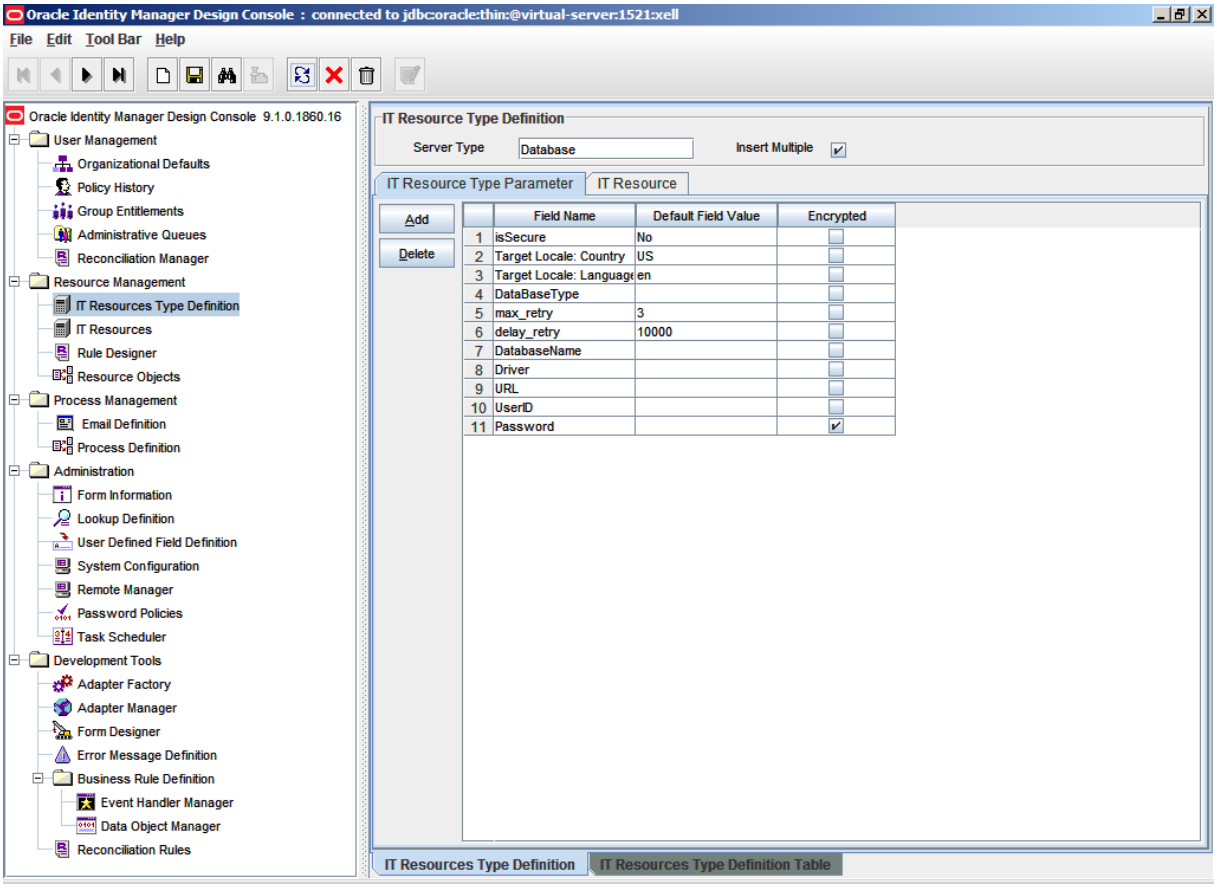
6.2.2.1. Vmesnik »Design Console«

Je zmogljiv, na programskem jeziku Java temelječ vmesnik za razvijalce in sistemske administratorje. Po namestitvi odjemalca »Design Console« nas na namizju pričaka ikona s katero zaženemo vmesnik. Po vnosu avtentikacijskih podatkov nas pričaka glavno okno vmesnika, kot ga prikazuje »Slika 6.3«.

V glavno oknu programa je na voljo pet kategorij z orodji za administriranje:

- »User Management«
- »Resource Management«
- »Process Management«
- »Administration«
- »Development Tools«

Glede na uporabniške pravice določene s strani administratorja, so lahko nekatere funkcije posameznih kategorij, opisane v nadaljevanju, onemogočene.



Slika 6.3: Glavno okno uporabniškega vmesnika »Design Console«

»User Management«:

Pod kategorijo »User Management« *(slov. upravljanje uporabnikov),* spadajo orodja namenjena sistemskim administratorjem za ustvarjanje in upravljanje informacij o organizaciji, uporabnikih, uporabniških skupinah, zahtevah, predlogah obrazcev, lokacijah,itn. Na voljo so naslednji obrazci:

- *»Organizational Defaults«:*

  Preko tega obrazca, lahko upravljamo z zapisi, ki odražajo notranjo strukturo organizacije in dodeljujemo vire na ravni celotne organizacije.

- *»Policy History«:*

  Obrazec omogoča vpogled v zapise o dovoljenjih za dostop do virov, ki so bili dodeljeni ali odvzeti določenemu uporabniku.

- *»Group Entitlements«:*

  Omogoča nastavljanje pravic dostopa za skupine uporabnikov, s katerimi določimo katere funkcionalnosti vmesnika »Design Console« bodo omogočene oziroma onemogočene.

- *»Administrative Queues«:*

  Obrazec omogoča ustvarjanje in upravljanje množičnega dodeljevanja privilegijev skupinam uporabnikov, za druge obrazce vmesnika »Design Console«

- *»Reconciliation Manager«:*

  Preko tega obrazca upravljamo uskladitvene dogodke *(ang. reconciliation events)* v OIM. Omogoča ogled, analizo, urejanje, povezovanje in upravljanje parametrov uskladitvenih dogodkov, prejetih iz ciljnih ter zaupanja vrednih virov.

»Resource Management«:

Pod kategorijo »Resource Management« *(slov. upravljanje z viri),* spadajo orodja za upravljanje z viri OIM. Na voljo so naslednje zaslonske maske:

- *»IT Resources Type Definition«:*

  Obrazec za ustvarjanje različnih tipov informacijskih virov. Vsak vir mora biti klasificiran. Vir je samo primerek tipa vira. Kot primer si lahko predstavljamo tip vira: »Database«, primerki tega tipa vira so pa lahko recimo: »Oracle imeDB-1«, »Microsoft SQL Server 2008 imeDB-2«. Tukaj najprej ustvarimo nov tip vira, šele nato lahko ustvarimo dejanski vir z obrazcem: »IT Resources«.
- *»IT Resources«:*

  Obrazec za upravljanje in konfiguracijo informacijskih virov. Vsak vir je primerek nekega tipa vira. Nastavitve definirane tukaj določajo kje se nek vir nahaja in kako naj OIM dostopa do njega.
- *»Rule Designer«:*

  Preko tega obrazca se nastavljajo različna pravila, ki se lahko nanašajo na varnostno politiko gesel, avtomatsko članstvo v skupinah, oskrbovanje uporabnikov, dodeljevanje nalog, itn.
- *»Resource Objects«:*

  Tukaj kreiramo in upravljamo objekte informacijskih virov. Primer objekta IT vira bi lahko bila recimo tabela podatkovne baze.

»Process Management«:

Nudi orodja za upravljanje in ustvarjanje OIM procesov ter kreiranje e-poštnih predlog za obvestila. Na voljo sta obrazca »Email Definition« in »Process Definition«

»Administration«:

Tukaj so zbrana orodja za upravljanje OIM administracijskih funkcij. Nudi naslednje obrazce: »Form Information«, »Lookup Definition«, »User Defined Field Definition«, »System Configuration«, »Remote Manager«, »Password Policies« in »Task Scheduler«.

»Development Tools«

Je paket razvojnih orodij, ki omogočajo skrbnikom sistema ali razvijalcem, da prilagodijo OIM.
Ta kategorija vsebuje naslednja orodja: »Adapter Factory«, »Adapter Manager«, »Form Designer«,

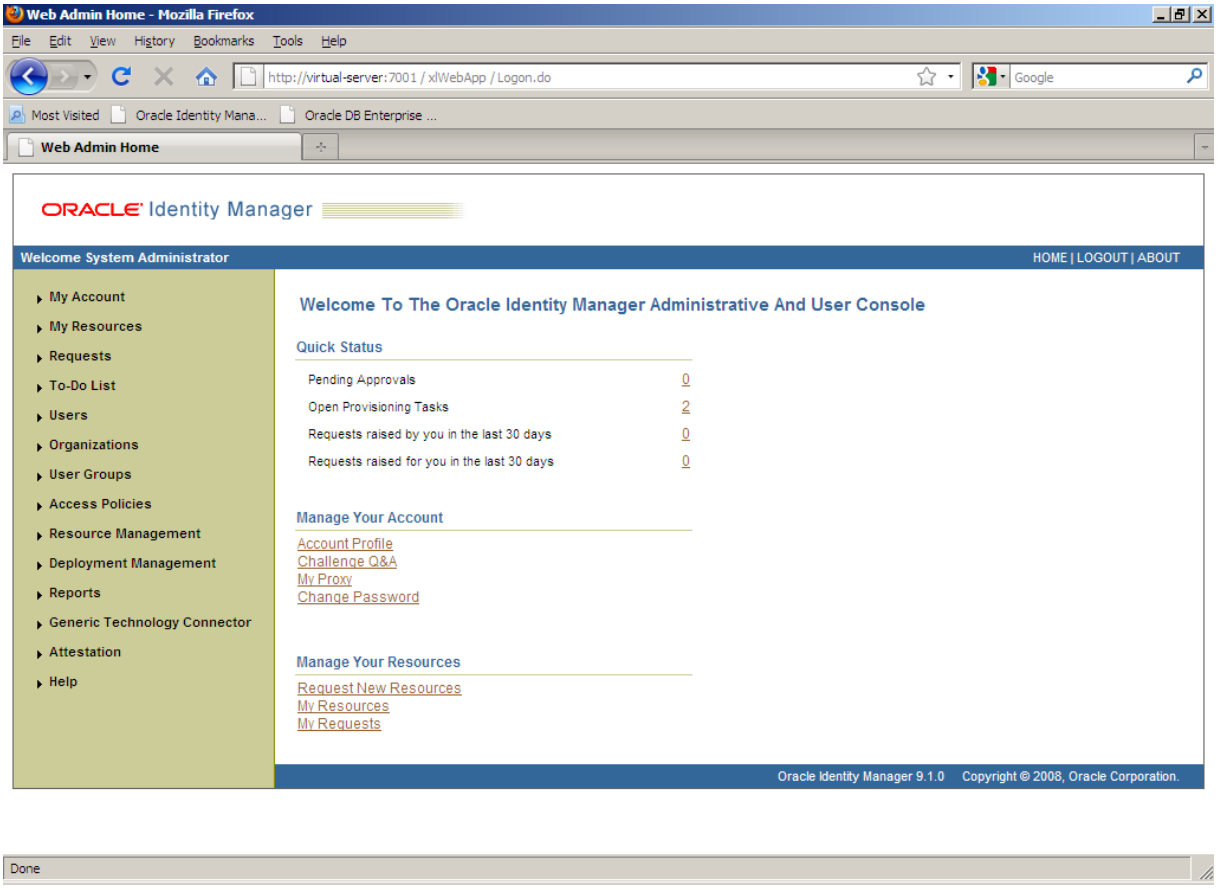
»Error Message Definition«, »Bussiness Rule Definition« in »Reconciliation Rules«.

6.2.2.2. Vmesnik »Administration and User Console«

Je spletni upravljavski vmesnik za administratorje identitet in končne uporabnike.

Dostop do spletnega vmesnika je mogoč preko naslova: `http://<hostname>:<port>/xlWebApp`

Pri čemer je `<hostname>` ime ali IP naslov računalnika na katerem gostuje aplikacijski strežnik, `<port>` pa številka vrat na katerih le-ta posluša za zahtevami.



Slika 6.4: Osnovna stran spletnega vmesnika: »Administration and User Console«

Na spletni strani nas pričaka okno za prijavo. V kolikor že imamo dostop se prijavimo, druga možnost, ki nam jo vmesnik ponuja pa je samopostrežna registracija, v kolikor dostopa še nimamo. Po prijavi, kot administrator nas pričaka glavno okno vmesnika, kot ga prikazuje »Slika 6.4«.

V glavno oknu programa je na voljo štirinajst kategorij z orodji za administriranje:

»My Account«:

Kategorija kjer spreminjamo in upravljamo osnovne podatke, povezane s svojim uporabniškim profilom, kot je recimo spreminjanje gesla in ostalih osebnih podatkov.

»My Resources«:

Upravljanje z informacijskimi viri, ki so nam bili dodeljeni, možnost vložitve novih zahtev za dostop do virov v lastnem ali drugem imenu.

»Requests«:

Možnost sledenja in upravljanja z zahtevki za dodeljevanje virov, ki smo jih ustvarili, oziroma smo za njih odgovorni. Upravljanje z nalogami, ki so nam bile dodeljene.

»To-Do List«:

Vsebuje seznam nalog v procesu oskrbovanja uporabnikov, ki jih moramo dokončati/odobriti. Naloge so sestavni elementi postopkov za odobritev zahtevkov in z njimi povezanih sredstev in virov, ki so na voljo pri oskrbovanju uporabnikov.

»Users«:

Vsaka identiteta, ki obstaja v sistemu OIM in se upravlja preko OIM, se imenuje »OIM User«. Tukaj kreiramo in upravljamo uporabnike.

»Organizations«:

Tukaj ustvarjamo in upravljamo organizacijsko strukturo organizacije. Oddelke, podjetja, podružnice, itn.

»User Groups«:

Skupine uporabnikov se uporabljajo za ustvarjanje in vodenje evidenc združevanja uporabnikov, ki jim želimo dovoliti dostop do skupnih funkcij, kot so pravice dostopa, vloge ali dovoljenja.

»Access Policies«:

Urejanje in ustvarjanje dostopnih politik. Dostopne politike so v bistvu seznami skupin uporabnikov in virov do katerih imajo te skupine dovoljenje za dostop.

»Resource Management«:

Upravljanje z informacijskimi viri na ravni organizacije ali za posameznika.

»Deployment Management«:

Je orodje za izvoz in uvoz OIM konfiguracije. Uporabno v primeru migracije namestitve sistema. Tukaj namestimo tudi vgrajene adapterje za povezavo z oddaljenimi viri.

»Reports«:

Orodje za ustvarjanje poročil z operativnimi in zgodovinskimi podatki. Tako ustvarjena poročila zagotavljajo informacije o virih, ki so na voljo uporabnikom v okviru OIM sistema.

»Generic Technology Connector«:

Namestitev in upravljanje generičnih konektorjev za povezavo z oddaljenimi viri.

»Attestation«:

Je mehanizem s katerim lahko nastavimo, da so uporabniki zadolženi za pregledovanje poročil periodično obveščeni o novih dodelitvah virov uporabnikom. Pregledovalci lahko tudi potrjujejo ali ima določen uporabnik pravico za dostop do vira.

6.2.3. Implementacija scenarija problemske domene z OIM

Kot je razvidno iz arhitekture scenarija problemske domene (»Slika 6.1« iz začetka poglavja) je logično zaporedje dogodkov pri implementaciji izbranega scenarija, da se sistem za oskrbovanje uporabnikov OIM najprej poveže z avtoritativnimi identitetnim virom (podatkovno bazo) in šele nato z Microsoft AD. V nadaljevanju bom opisoval zaporedje korakov, ki so bili potrebni pri implementaciji scenarija problemske domene v okolju OIM. Pri tem bom komentiral svoje izkušnje, ki sem jih pridobil ob uporabi tega sistema.

6.2.3.1. Namestitev konektorja za povezavo z Oracle Database 10g

Oracle je ubral pri tako imenovanih »že vgrajenih« konektorjih za povezavo z oddaljenimi sistemi zanimiv pristop, saj konektorji niso »fizično« vgrajeni v sistem. Kadar je govora o vgrajenih konektorjih pri Oraclu, to pomeni da so le-ti certificirani s strani Oracla za uporabo v navezavi z določenim oddaljenim podatkovnim virom, namestiti pa jih je treba ročno. S tem so uporabnike prisilili, da vedno uporabljajo najnovejše konektorje. Pred namestitvijo jih je namreč potrebno prenesti iz spletne strani proizvajalca[1].

Kakor je razvidno iz »Tabele 5.2«, sem za povezavo z relacijsko podatkovno bazo Oracle Database 10g moral namestiti konektor »Database Application Tables«, verzije 9.1.0.2. Isti konektor služi tudi za povezavo s podatkovnimi bazami proizvajalcev IBM in Microsoft. Ob vsaki izdaji konektorja Oracle izda tudi tehnično dokumentacijo[2] za dotični konektor. Branje omenjene dokumentacije je za popolnega začetnika, kakor sem bil sam ob prvem stiku s sistemom precej zahtevno, saj privzema, da imamo predhodno znanje za delo s sistemom OIM.

Kot omenjeno zgoraj, je pred namestitvijo konektorja le-tega potrebno prenesti s spletne strani proizvajalca. Stisnjeno datoteko se razpakira v:`\OIM_HOME\xellerate\ConnectorDefaultDirectory` direktorij. Kadarkoli se dodaja ali briše vsebino zgoraj omenjenega direktorija je potrebno vsebino, ki

[1] http://www.oracle.com/technology/software/products/ias/htdocs/connectors.html
[2] http://download.oracle.com/docs/cd/E11223_01/index.htm

se nanaša na konektorje izbrisati iz predpomnilnika strežnika OIM. To naredimo z zagonom skripte kot jo prikazuje naslednja vrstica:

```
\OIM_HOME\xellerate\bin\PurgeCache.bat ConnectorResourceBundle
```

Dejanska namestitev adapterja poteka preko spletnega administracijskega vmesnika »Administration and User Console«, ki je bil opisan v »poglavju 6.2.2.2.«. V meniju izberemo opcijo »Deployment Management«, ki je primarno namenjena nameščanju adapterjev za povezavo z oddaljenimi viri in uvozu ter izvozu OIM konfiguracij. Tam nas pričaka pod opcijo »Install Connector« namestitveni čarovnik, ki nas na uporabniku prijazen način vodi skozi namestitveni postopek. O konfiguraciji pravkar nameščenega konektorja pišem v nadaljevanju.

6.2.3.2. Ustvarjanje povezave s PB - postavitev GTC konektorja

Ustvarjanje povezave s podatkovno bazo in preslikava atributov iz tabele v atribute OIM sistema prav tako poteka preko spletnega administracijskega vmesnika »Administration and User Console«. V meniju tokrat izberemo opcijo »Generic Technology Connector«, kje se namešča in upravlja z generičnimi konektorji za povezavo z oddaljenimi viri. Tudi tukaj nas pričaka ličen konfiguracijski čarovnik.

Eden pomembnejših parametrov, ki jih je potrebno določiti takoj na začetku postopka, je način delovanja v katerem želimo, da deluje naš GTC konektor. Terminologija med izdelovalci se tukaj deloma razlikuje, zato bom na tem mestu predstavil kako Oracle definira različne načine delovanja za svoje konektorje:

Usklajevanje (ang. Reconciliation):

Usklajevanje je proces kjer OIM pridobiva informacije iz oddaljenega podatkovnega vira.

Usklajevanje s ciljnim virom (ang. Targeted resource reconciliation):

Usklajevanje s ciljnim virom vključuje pridobivanje informacij, o na novo ustvarjenih ali spremenjenih uporabnikih, iz ciljnega sistema in uporabo teh podatkov za dodajanje ali spreminjanje virov, ki so dodeljeni uporabniškemu računu (uporabniški identiteti) v okviru OIM sistema. V kolikor uporabnika v OIM sistemu ne najde, uporabniškega računa zanj tudi ne bo ustvarilo. Torej imamo v ciljnem sistemu osiroteli uporabniški račun *(ang. orphan account).*

Zaupno usklajevanje z virom (ang. Trusted source reconciliation):

Podpira kateregakoli izmed spodaj naštetih scenarijev, ki se lahko zgodijo ob sprožitvi zaupnega usklajevanja z virom:

- Za vsakega na novo ustvarjenega uporabnika na ciljnem sistemu, se ustvari uporabniški račun tudi v OIM sistemu.
- Vse posodobitve, ki se zgodijo nad uporabnikom v ciljnem sistemu zazna tudi OIM in uskladi vse spremembe z uporabniškim računom v OIM sistemu.

Oskrbovanje uporabnikov (ang. Provisioning):

Oskrbovanje uporabnikov je proces, kjer OIM pošilja informacije ciljnim podatkovnim virom. Konektor, ki sem ga namestil podpira funkcije ustvarjanja, spreminjanja, omogočanja, onemogočanja in izbrisa uporabniškega računa.

Večina »že vgrajenih« konektorjev, ki jih podpira OIM lahko delujejo v vseh zgoraj opisanih načinih.

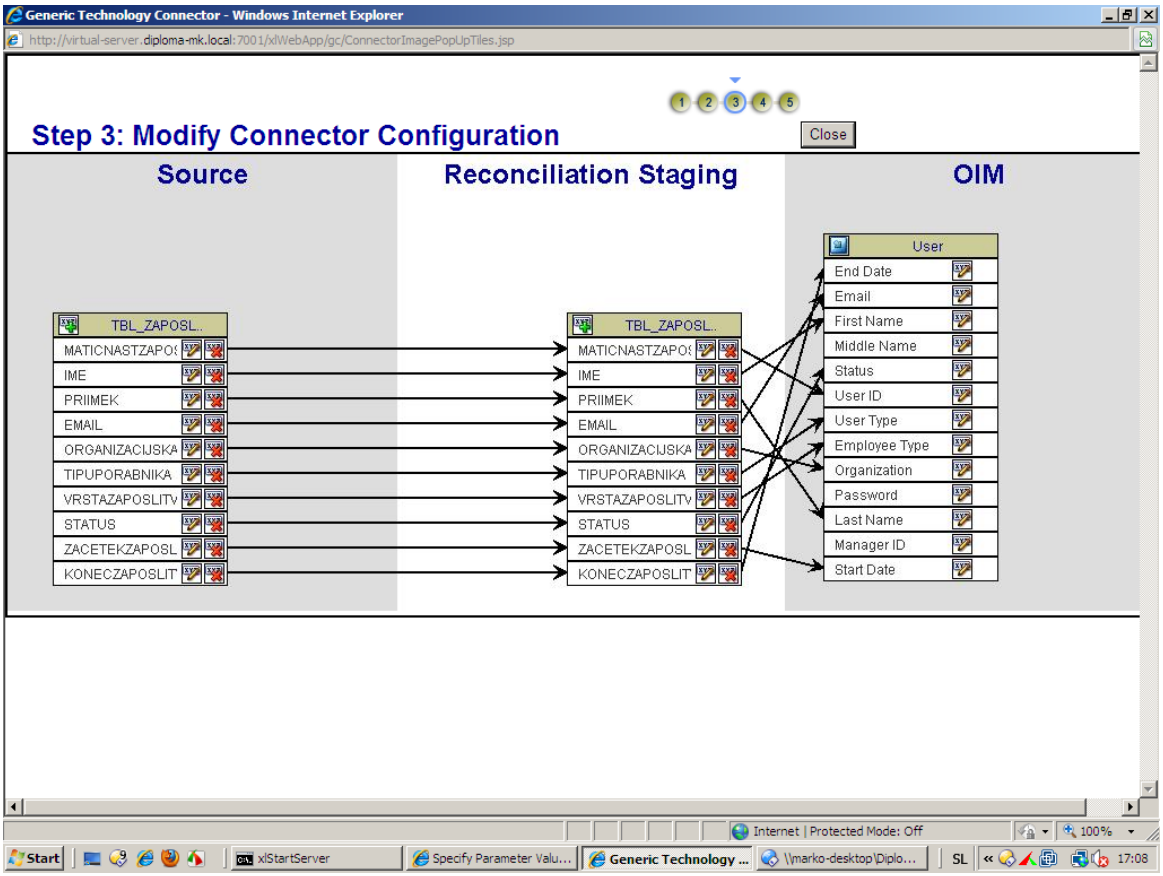
V definiciji problemske domene sem tabelo v podatkovni bazi določil kot avtoritativni vir identitetnih informacij - zato je bila na tem mestu moja izbira - zaupno usklajevanje z virom. Med pomembnejšimi nastavitvami, ki jih je potrebno definirati v konfiguracijskem čarovniku je tip JDBC gonilnika za podatkovno bazo in pa URL naslov kje se nahaja podatkovna baza do katere želimo dostopati. Pri tem je pomembno omeniti, da mora biti URL naslov prav tako v JDBC formatu. V mojem testnem primeru, kjer sem uporabil kar Oracle JDBC gonilnik je JDBC URL naslov izgledal takole: `jdbc:oracle:thin:@virtual-server:1521:xell`

Izbrati je potrebno še korensko tabelo, kjer se nahajajo podatki na podlagi katerih bomo delali preslikavo in pa morebitno odvisno podtabelo, ter seveda vnesti še vse ostale zahtevane parametre z ustreznimi avtentikacijskimi podatki za dostop do podatkovne baze.

V kolikor je bila konfiguracija parametrov za dostop do tabele podatkovne baze uspešna, nas v tretjem koraku čarovnika pričaka zaslon, kot ga prikazuje »Slika 6.5«. Sistem OIM s pomočjo podanih parametrov prebere metapodatke in naredi začetno preslikavo iz stolpcev tabele podatkovne baze v tako imenovani »Reconciliation Staging data set«.Ta »data set« nosi uporabniške podatke, ki sta jih pred tem obdelala validacijski in transformacijski modul GTC konektorja.

V tem koraku lahko dodajamo, spreminjamo ter brišemo parametre preslikave. Prav tako lahko spremenimo tip atributa; recimo datum, ki ga je GTC konektor označil kot »String« spremenimo v tip »Date« itn. Najpomembnejše opravilo tega koraka v čarovniku za ustvarjanje povezave pa je določitev preslikave »data seta« iz »Reconciliation Staging« v »OIM Staging«. Ta postopek je zelo intuitiven, saj že iz imena atributov vidimo katere atribute tabele je potrebno povezati k atributom OIM uporabniškega računa.

Vsaka identiteta, ki obstaja v sistemu OIM in se upravlja preko OIM, se imenuje »OIM User«. Pri tem ni odveč poudariti, da so nekateri atributi pri ustvarjanju uporabniškega računa v OIM sistemu obvezni. Ti atributi so »User ID«, »First Name«, »Last Name«, »Employee Type«, »User Type« in pa »Organization«.



Slika 6.5: Preslikava stolpcev tabele v atribute OIM sistema

Na tem mestu bom omenil še atribut »Status«, ki ga je potrebno samo preslikati v atribut z istim imenom na OIM sistemu. Njegovo funkcionalnost ima OIM sistem že implementirano. Brez, da bi karkoli programirali, je logika za kreiranje, brisanje in onemogočanje uporabniške identitete v OIM sistemu izvedena preko vrednosti tega atributa. To pomeni da je »OIM User« aktiven ob vrednosti »Status« atributa »Active«, onemogočen ko je le ta »Disabled« in izbrisan ko je le-ta »Deleted«.

Na podlagi zgoraj opisane funkcionalnosti lahko na enostaven način, brez programiranja ustvarjamo, brišemo in onemogočamo uporabnike v vseh odvisnih identitetnih virih, priklopljenih na OIM.

6.2.3.3. Izvajanje zaupnega usklajevanje s PB

V prejšnjem podpoglavju sem prikazal kako ustvarimo povezavo s PB. Sedaj je na vrsti izvajanje usklajevanja na podlagi te povezave. V spletnem administracijskem vmesniku se v meniju

pomaknemo v kategorijo »Resource Management«. Tukaj se med drugim nahaja tudi podkategorija »Managed Scheduled Tasks« ali po slovensko »Razporejevalnik opravil«. Ob tem, ko smo ustvarili povezavo s PB v prejšnjem poglavju se je avtomatsko generiralo tudi opravilo zanj. Izberemo opravilo, ki ima imenu določenem v prejšnjem podpoglavju dodano končnico »GTC«. Tukaj nastavimo urnik izvajanja zaupnega usklajevanja z našim avtoritativnim identitetnim virom. Izvajanje je lahko ročno, lahko pa ga popolnoma avtomatiziramo z nastavitvijo ure ob kateri se naj proži ter intervalov ponavljanja.

6.2.3.4. Namestitev konektorja in ustvarjanje povezave z AD

Namestitev konektorja za ustvarjanje povezave z Microsoftovim AD je podobna namestitvi opisani »poglavju 6.2.3.1.«, zato bom tukaj samo omenil, da sem namestil »Microsoft Active Directory User Management v9.1.1.1« konektor, ki ga je prav tako potrebno prenesti iz spletne strani proizvajalca.

Ustvarjanje povezave pa ni analogno kot v »poglavju 6.2.3.2«. V spletnem administracijskem vmesniku izberemo kategorijo »Resource Management« in nato podkategorijo »Manage IT Resource«. Pri ustvarjanju povezave nam tudi tokrat pomaga namestitveni čarovnik za ustvarjanje »IT vira«. Med pomembnejšimi parametri, ki jih potrebno vnesti so seveda avtentikacijski podatki za uporabnika z administracijskimi pravicami dostopa do AD domene ter »Distinguished Name« za moj testni primer, kjer želimo upravljati z uporabniškimi identitetami (dc=diploma-mk,dc=local).

Posebnost tega konektorja je v tem, da lahko njegove zmožnosti delovanja razširimo z uporabo oddaljenega konektorja oziroma agenta (ang. remote agents). Takšen tip konektorja sem omenil v »poglavju 3.4.1.1.d«. Z namestitvijo tega oddaljenega konektorja na strežniku, kjer se nahaja ciljni vir dobimo v obeh načinih delovanja (oskrbovanje in uskladitev) možnost, da se z OIM sistemom usklajujejo tudi atributi, ki se nanašajo na »Terminal Services Profile« posameznega uporabnika v Microsoft AD domeni.

Pred prvim izvajanjem oskrbovanja uporabnikov z novim virom, torej kreiranjem uporabnika v AD domeni, je potrebno v upravljalniku opravil dodeliti pravkar ustvarjeni »IT vir« za naslednja opravila: »AD Group Lookup Recon« in »AD Organization Lookup Recon«. Le-ti sta bili ob namestitvi konektorja avtomatsko ustvarjeni. S tem uvozimo strukturo AD sheme v OIM, uporabniške skupine ter organizacije. To nam omogoča, da uporabnika dodelimo v točno določeno uporabniško skupino in organizacijo znotraj AD domene.

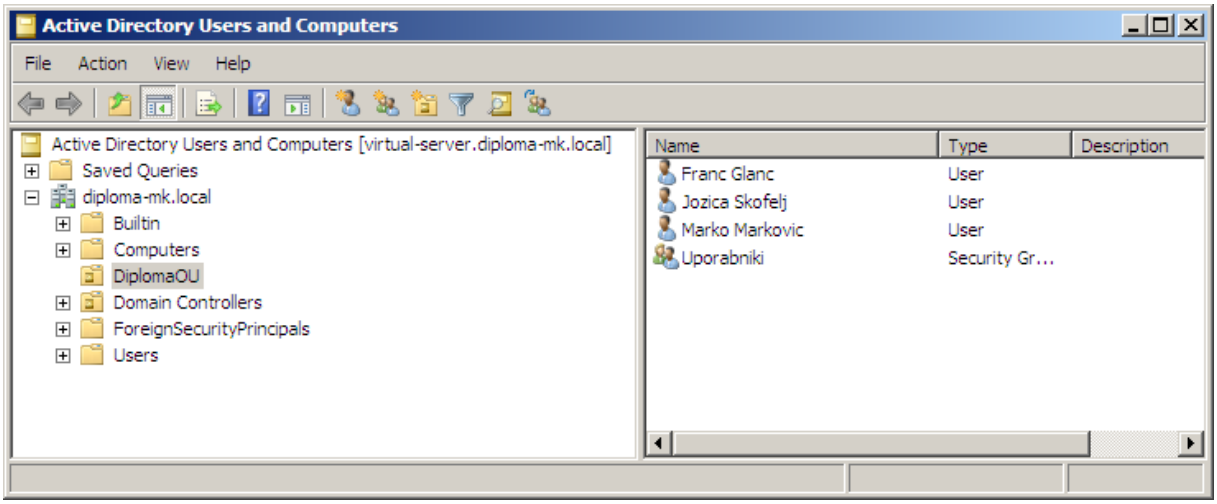
6.2.3.5. Ustvarjanje uporabnikov v AD domeni

Konfiguracija OIM sistema opisana v prejšnjih podpoglavjih nam sedaj omogoča ročno izvajanje scenarija, kot ga opisuje definirana problemska domena iz »poglavja 6.1.«. To pomeni, da je

potrebno vsakega uporabnika, ki ga uvozimo iz tabele podatkovne baze v OIM sistem ročno oskrbeti z AD virom in šele nato se uporabniški račun ustvari tudi v AD domeni.

Za avtomatizacijo opisanega postopka je potrebno ustvariti še novo dostopno politiko *(ang. Access Policy)* v OIM sistemu. Dostopne politike so v bistvu seznami skupin uporabnikov in virov do katerih imajo te skupine dovoljenje za dostop.

Tudi to opravilo izvedemo preko spletnega administracijskega vmesnika in sicer v kategoriji »Access Policies«. Že dobro znan postopek s čarovnikom nas vodi skozi potrebne nastavitve parametrov. Izberemo možnost, da ne želimo odobritve s strani nadrejenega uporabnika oziroma administratorja.



Slika 6.6: Ustvarjeni uporabniki v AD domeni

Ostale nastavitve parametrov so dokaj trivialne, ker nastavljanje le-teh čarovnik zelo olajša. Na tem mestu naj omenim, da sem pri nastavitvi dostopnih politik moral uporabiti tudi administracijski vmesnik »Design Console«, kjer sem na obrazcu za ustvarjanje uporabnikov vklopil funkcijo za samodejno shranjevanje obrazca pri ustvarjanju uporabnikov v AD domeni.

6.3. Microsoft Identity Lifecycle Manager 2007 FP1

6.3.1. Namestitev

Namestitev ILM je v primerjavi z OIM dokaj trivialno opravilo, saj je osredotočena na Microsoftove produkte. S tem odpade veliko število različnih možnih namestitev. Pred namestitvijo ILM je tako potrebno namestiti samo relacijsko podatkovno bazo in pa .NET Framework 2.0 ali novejši, v kolikor že nista nameščena. Za optimalno delovanje je priporočeno, da ILM namestimo na isti strežnik kot SQL Server, ki ga le-ta potrebuje za svoje delovanje, v nasprotnem primeru izgubimo precej

performansov[**13**]. Sam sem se odločil, da za repozitorij ILM-ja uporabim Microsoft SQL Server 2008, čeprav ni uradno certificiran s strani Microsofta, sem na uradnih forumih izdelka prebral, da takšna namestitev deluje brezhibno.

Kot je razvidno iz »poglavja 5.2.3«, ima ILM 2007 FP1 dva bistvena sestavna dela. Takšna je tudi namestitev, saj nam namestitveni čarovnik ponudi dve možnosti namestitve:

- Meta imenik in funkcionalnosti oskrbovanja uporabnikov ali pa:
- Upravljanje s certifikati in pametnimi karticami

Namestil sem samo prvo možnost, ker je bila le-ta tudi predmet testiranja v scenariju problemske domene. Namestitev je bila v primerjavi z OIM sistemom zelo trivialna, saj namestitveni čarovniki poskrbijo za vse ključne nastavitve, zato je ne bom podrobneje opisoval. Po končani namestitvi poteka vse upravljanje preko samo enega administracijskega vmesnika, ki je predstavljen v nadaljevanju.

6.3.2. Administracijski vmesnik

V administracijskem vmesniku, kot ga prikazuje »Slika 6.7« je na voljo pet zavihkov z različnimi orodji:

- »Operations«
- »Management Agents«
- »Metaverse Designer«
- »Metaverse Search«
- »Joiner«

»Operations«:

V zavihku »Operations« se shranjujejo rezultati vsake izvršitve izvajalnih profilov »Management Agent-ov«. Tukaj lahko pregledujemo zgodovino določenih akcij, ki so se zgodile ob sprožitvi posameznega agenta, npr. ali je bila sinhronizacije uspešna. Gre v bistvu za dnevnik dogodkov.

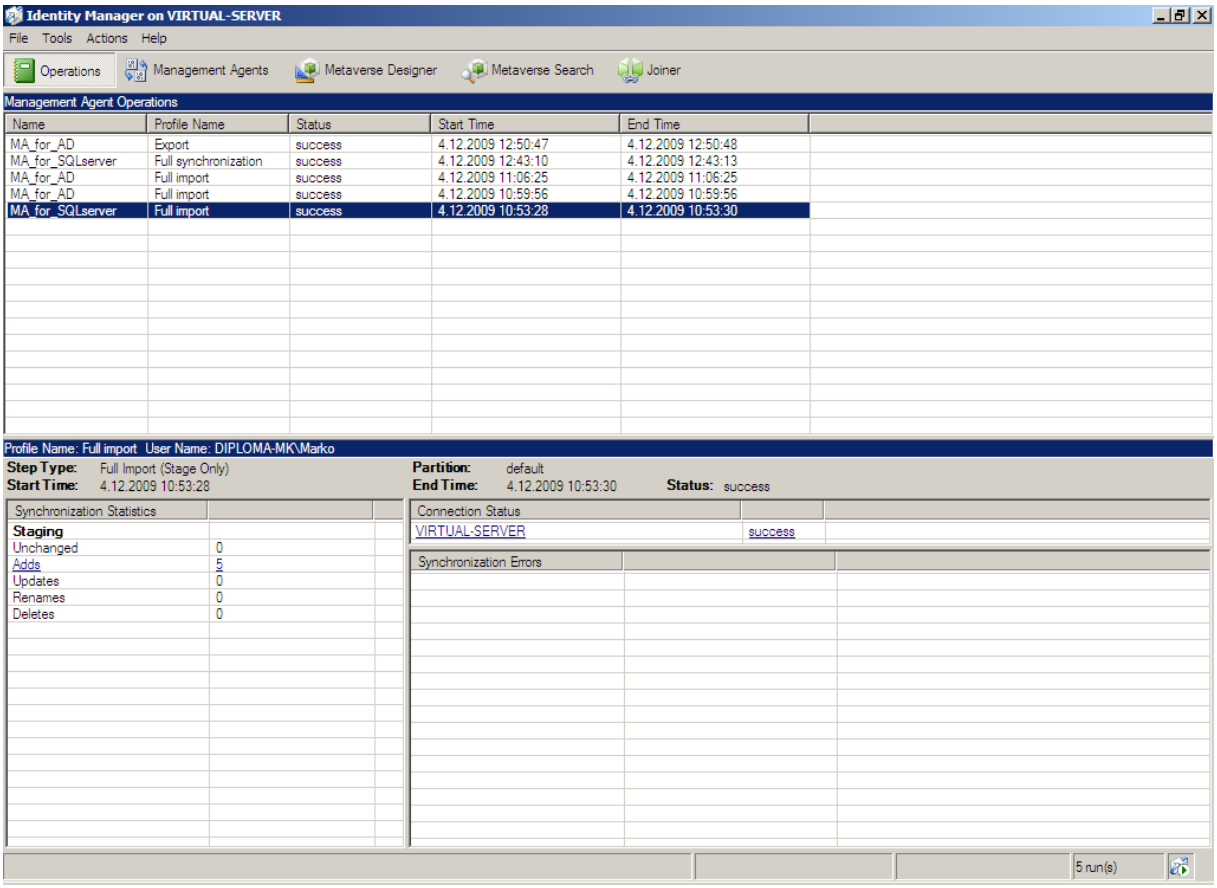
»Management Agents«:

V zavihku »Management Agents« ustvarjamo povezave z oddaljenimi podatkovnimi izvori. MA izvajajo operacije izvoza in uvoza podatkov iz kateregakoli priklopljenega CS v ILM-jev Metaverse ter sinhronizacijo teh podatkov v njem.

»Metaverse Designer«:

Metaverse se v ILM imenuje meta imenik. Metaverse Designer se uporablja za ustvarjanje in nastavljanje tipov objektov in njihovih atributov. ILM ustvari svojo lastno metaverse shemo, ki

opredeljuje tipe objektov, kot je npr. oseba ali organizacija, in nabor atributov, ki so povezane z vsakim tipom objekta v MV shemi.



Slika 6.7: Administracijski vmesnik ILM 2007 FP 1.

»Metaverse Search«:

Se uporablja za iskanje, pregledovanje in nastavitve stanja objektov v »Metaverse« oziroma meta imeniku.

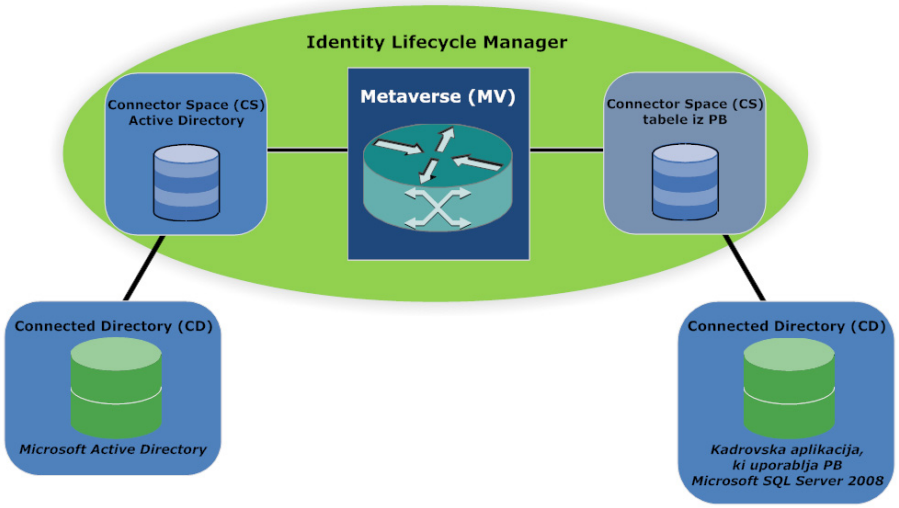
»Joiner«:

»Joiner« se uporablja za iskanje in pregled objektov, ki niso povezani z »metaverse objekti«. Iskanje lahko vrne vse vrste ali pa samo določene tipe objektov. »Joiner« se nato uporabi za ročno preslikovanje oziroma povezovanje določenega objekta iz CS z »metaverse« objektom.

6.3.3. Implementacija scenarija problemske domene z ILM

Tudi z Microsoftovim sistemom za oskrbovanje uporabnikov sem se lotil implementacije izbranega scenarija problemske domene, kot ga prikazuje »Slika 6.1« iz začetka tega poglavja. V nadaljevanju bom opisoval zaporedje korakov, ki so bili potrebni pri implementaciji le-tega v okolju sistema ILM. Pri tem bom komentiral svoje izkušnje, pridobljene ob uporabi tega sistema.

»Slika 6.8« prikazuje pretok objektov scenarija problemske domene pri implementaciji z ILM sistemom. Za boljše razumevanje v nadaljevanju obravnavnih področij je nujno razumevanje osnovne ILM terminologije, ki sem jo predstavil v »poglavju 5.2.3.« tega dela.



Slika 6.8: Pretok objektov scenarija problemske domene v okolju ILM sistema

6.3.3.1. Ustvarjanje povezave s PB

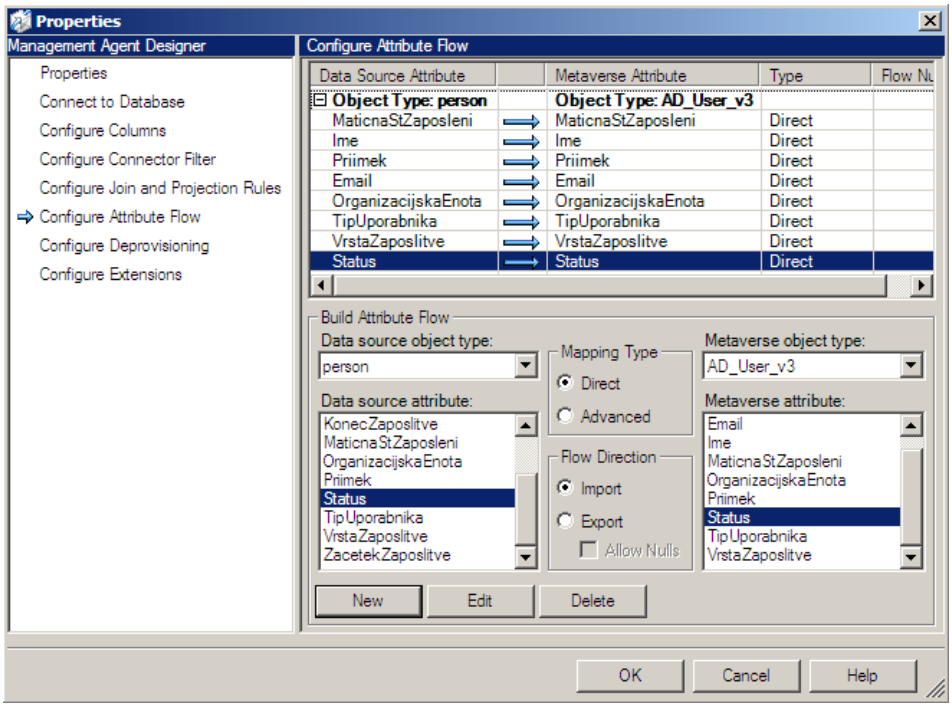
Microsoft se za razliko od OIM sistema pri vgrajenih konektorjih dobesedno drži besede »vgrajeni«, saj le-teh ni potrebno naknadno prenašati iz spletne strani proizvajalca. Smo pa seveda s tem prikrajšani ob morebitne nadgradnje le-teh.

Za povezavo z oddaljenimi podatkovnimi viri (»Connected Directory« ali CD)pri ILM skrbijo tako imenovani »Management Agents«. Vse nastavitve, ki se tičejo konfiguriranja povezav s CD-ji se tako opravljajo v zavihku z istim imenom. Tudi v ILM nas ličen konfiguracijski čarovnik vodi čez postopek ustvarjanja podatkovne baze.

Čarovnik je razdeljen na osem korakov, ki jih je potrebno izvesti tekom postopka ustvarjanja povezave s PB. Prva dva koraka sta namenjena vnašanju standardnih parametrov, kot so naslov strežnika in podatkovna baze, imena tabele ter avtentikacijskih podatkov. Večjo pozornost je potrebno nameniti tretjemu koraku »Configure Columns«, kjer nam ILM pokaže atribute iz tabele. Na tem mestu je potrebno označiti primarni ključ po katerem se razlikujejo naše identitete in pa definirati tip objekta s katerim bodo identitete vira zastopane v ILM, recimo da je to »person«. Naslednji korak »Configure Connector Filter« služi definiranju kriterijev določenih objektov, ki jih ne bi želel uvoziti.

Za boljše razlikovanje kateri objekt spada v MV in kateri je tip objekta vira PB, sem z »Metaverse Designer-jem« kreiral nov tip MV objekta »AD_User« in izbral atribute, ki jih naj ima. Nato v naslednjem koraku kreiranja povezave - »Configure Join and Projection Rules« izberemo preslikavo iz »person« v »AD_User«.

»Slika 6.9« prikazuje konfiguracijski čarovnik v koraku »Configure Attribute Flow«, ki je namenjen preslikovanju atributov tipa »person« iz tabele PB v tip »AD_User« MV objekta. Določiti je potrebno smer preslikave, torej v mojem primeru »Import« iz PB v meta imenik.



Slika 6.9: Preslikava stolpcev tabele v atribute ILM sistema

V predzadnjem koraku ustvarjanja povezave s PB - »Configure Deprovisioning« določimo kaj se zgodi v primeru, ko je objekte potrebno izbrisati. Ker je v scenariju problemske domene tabela v PB avtoritativni vir podatkov je potrebno samo izbrati opcijo »Make them disconnectors«. S tem prekinemo preslikavo objekta iz CS podatkovne baze v MV objekt. Vendar ta nastavitev ni dovolj, saj smo sedaj samo izbrisali prej omenjeno preslikavo objektov. V zavihku »Metaverse Designer« je potrebno za tip MV objekta »AD_User« nastaviti še pravilo, ki določa, da bo izbrisan tudi MV objekt, ko bo preslikava prekinjena.

Zadnji korak - »Configure Extensions« je namenjen vstavljanju ročno napisanih programskih dodatkov. V kolikor to želimo je potrebno uporabiti »Microsoft Visual Studio«. S kodiranjem lahko potem bolj specifično določamo kaj vse se dogaja z atributi pri povezavi s PB.

6.3.3.2. Ustvarjanje povezave z AD

Ustvarjanje povezave z AD je podobno tistemu iz prejšnjega podpoglavja. Omenil bom samo razlike. Namestitveni čarovnik nas vodi skozi deset korakov. Prvi trije koraki so dokaj trivialni. Namesto tabele v podatkovni bazi izberemo vsebnik v AD domeni kjer bodo shranjeni uporabniki (DC=diploma-mk, DC=local, OU=DiplomaOU) ter vpišemo ustrezne avtentikacijske podatke. V četrtem koraku - »Select Object Types« nam ILM na podlagi AD sheme, v izbor ponudi tipe objektov, ki jih želimo uveljavljati pri preslikavi. Sledi »Select Object Types«, kjer ponovimo postopek iz prejšnjega koraka le, da tokrat izbiramo atribute, potrebne pri preslikavi našega MV objekta v AD objekt.

Koraka »Configure Connector Filter« in »Configure Join and Projection Rules«, kar izpustimo. Želimo namreč ustvariti vse objekte iz meta direktorija - saj gre za postopek dodeljevanja vira uporabniku.

Čaka nas še preslikovanje - »Configure Attribute Flow«. Atribute tipa »AD_User« MV objekta je potrebno preslikati v tip »user« AD objekta. Smer preslikave je seveda »Export«, saj gre za preslikavo iz meta direktorija v AD.

Definiramo še pravilo, ki določa kaj se zgodi v primeru, ko je objekte potrebno izbrisati - »Configure Deprovisioning«. Izbrati je potrebno opcijo »Stage a delete on the object for the next export run«. S tem ILM-ju povemo, da naj izbriše vse objekte iz AD, ki imajo prekinjeno preslikavo. To so preslikave objektov iz CS AD v MV objekt ILM-ja.

6.3.3.3. Kreiranje uporabniškega računa v AD

Pri implementaciji scenarija problemske domene se je pokazalo, da ima Microsoft ILM hudo pomanjkljivost, že pri tako tipičnih operacijah, kot je kreiranje uporabniškega računa v AD. To funkcionalnost je namreč potrebno ročno sprogramirati. Za to opravilo pa potrebujemo nameščen »Microsoft Visual Studio«. ILM podpira dva programska jezika iz ogrodja .net in sicer »Visual Basic« ter »C#«.

Programsko kodo potrebujemo zato, da najprej kreiramo uporabnika tipa »user« v »Connector Space-u« AD, in šele po izvajanju profila »Export« se uporabniški račun dejansko ustvari v AD. »Slika 6.8« iz začetka poglavja prikazuje pravkar opisani pretok objektov. Izvajalne profile bom pa razložil v naslednjem podpoglavju.

ILM sicer zgradi ogrodje, ki ga potrebujemo pri pisanju kode za »provision« akcije, še vedno pa logiko moramo sprogramirati sami. Ob brskanju po spletu sem naletel na orodje »MIIS resource kit«, ki je v bistvu čarovnik, ki bi naj omogočal avtomatsko generiranje kode za kreiranje uporabnikov v ciljnih sistemih. Z omenjenim orodjem, mi zaradi pomanjkljive dokumentacije, ni uspelo generirati kode, ki

bi mi ustvarila uporabnika v AD. Zelo nenavadna poteza Microsofta, da podobne funkcionalnosti niso vgradili v sam sistem. Posebej ob podatku, da izid prej omenjenega orodja datira v leto 2004, medtem ko je bila trenutna verzija ILM sistema splavljena na trg v letu 2007.

Ob pisanju kode za ustvarjanje uporabnikov v CS ciljnega sistema sem moral dodati še logiko za brisanje uporabnika iz AD v kolikor se spremeni vrednost atributa »Status« v avtoritativnem viru iz »Active« na »Deleted«. V tem primeru namreč uporabniku odvzamemo dostop do AD, z izbrisom njegovega uporabniškega računa.

6.3.3.4. Konfiguracija izvajalnih profilov za povezavo s PB in AD

Preden lahko začnemo s sinhronizacijo uporabniških identitet iz tabele podatkovne baze v AD je potrebno ustvariti še izvajalne profile za vsakega izmed konektorjev, ki smo ju ustvarili v prejšnjih poglavjih. To naredimo v zavihku »Management Agents« pod opcijo »Configure Run Profiles«.

Tako kot Oracle, tudi Microsoft uporablja svojstveno terminologijo pri določevanju načina v katerem lahko delujejo konektorji oziroma MA , zato v nadaljevanju sledi razlaga le-teh.

Full Import

Prebere vedno cel CD. Vsi objekti ter atributi iz oddaljenega podatkovnega vira se prenesejo v CS.

Delta Import

V kolikor je CD sposoben razlikovanja sprememb, kot je recimo AD, lahko iz CD dobimo samo objekte ter atribute, ki so se spremenili od zadnjega »Full Import-a«.

Full Synchronization

Sinhronizacija se izvede na vseh objektih, ki so shranjeni v CS. Pretok podatkov je tak, da se objekti iz CS najprej sinhronizirajo z MV objekti in nato tudi navzven z objekti iz vseh ostalih CS, ki imajo vezane objekte na isti MV objekt.

Delta Synchronization

Sinhronizacija se izvede samo na objektih ter atributih, ki so shranjeni v CS in so se spremenili. Pretok podatkov je podoben kot pri »Full Synchronization«. Razlika je le v tem, da se sinhronizirajo samo objekti iz CS, ki so se spremenili od zadnje sinhronizacije.

Export

Izvoz objektov ter atributov iz CS v CD. Izvoz je vedno tipa »delta«. Izvozijo se namreč samo objekti ter atributi iz CS, ki se razlikujejo od objektov ter atributov v oddaljenem podatkovnem viru.

Za izvajanje sinhronizacije scenarija problemske domene sem kreiral pet izvajalnih profilov. Za MA podatkovne baze: »Full Import«, »Full Synchronization« ter »Delta Synchronization«. Za AD pa profil tipa »Export« in »Full Import«.

6.3.3.5. Izvajanje sinhronizacije

Pri razumevanju izvajanja sinhronizacije uporabniških identitet iz tabele podatkovne baze v Microsoftov AD nam pomaga »Slika 6.8«, ki prikazuje pretok objektov scenarija problemske domene v okolju ILM sistema.

- Sinhronizacijski cikel začnemo z izvajanjem profila »Full Import« nad MA za SQL Server, kar prenese objekte iz avtoritativnega vira v CS tabele podatkovne baze.
- Potreben je prav tako »Full Import« AD strukture v njegov CS, kar izvedemo z izvajanjem MA profila za AD
- Šele sedaj pride na vrsto sinhronizacija objektov iz obeh CS znotraj meta imenika, imenovanega Metaverse. To naredimo z izvajanjem MA profila za SQL Server tipa »Full Synchronization«. S tem smo dejansko ustvarili preslikavo obeh tipov »user« in »person« v MV tip »AD_User«.
- Na vrsti je izvajanje profila tipa »Export« nad MA za Microsoft AD. V tem koraku ILM dejansko ustvari oziroma briše uporabnike iz strukture AD.
- Za potrditev sinhronizacijskega cikla je potreben še »Full Import« iz AD.

Pomanjkljivost sistema ILM je vsekakor tudi to, da je potrebno zgoraj prikazani scenarij vsakič izvajati ročno ali pa sprogramirati skripto, ki proces avtomatizira.

6.4. Povzetki primerjave

Oracle Identity Manager prekaša Microsoftov ILM tako na področju podprtih okolij, kakor tudi na področju števila vgrajenih *(ang. out of the box)* konektorjev. OIM je zahvaljujoč javanskemu značaju možno namestiti na tri različne operacijske sisteme (Windows, Linux, Solaris). Medtem, ko ILM teče samo na strežniški različici Windows operacijskega sistema. Tudi pri izbiri relacijske podatkovne baze, ki jo sistema uporabljata za interno shranjevanje metapodatkov, je OIM bolj neodvisen. Za repozitorij lahko namreč uporablja tako Oracle podatkovno bazo, kakor tudi Microsoftov SQL Server. ILM je omejen samo na slednjega.

Relativna neodvisnost OIM sistema od okolja na katerem deluje terja tudi svojo ceno. Za svoje delovanje namreč potrebuje tudi aplikacijski strežnik. To dejstvo dodatno zakomplicira namestitev in

konfiguracijo, saj podpira kar štiri različne izvedbe le-teh. Pri namestitvi je potrebno kar nekaj »ročnega« dela in branja dokumentacije preden sistem deluje kot mora. ILMjev izdelek deluje samo na hišnih, torej Microsoftovih izdelkih, zato je tudi namestitev v primerjavi z OIM res trivialno lahko opravilo.

	Podprta okolja	Vgrajeni konektorji	Zahtevnost namestitve
Oracle Identity Manager	Pestra izbira različnih kombinacij namestitev.	Veliko podprtih proizvajalcev.	Visoka.
Microsoft Identity Lifecycle Manager	Namestitev možna samo na Microsoftove izdelke.	Manjši nabor vgrajenih konektorjev za povezavo na oddaljene vire.	Nizka.

Tabela 6.1: Primerjalna tabela podprtih okolij, vgrajenih konektorjev in zahtevnosti namestitve

Preden sem se lotil primerjave obeh sistemov na podlagi implementacije scenarija problemske domene nisem imel izkušenj z nobenim izmed primerjanih sistemov. Tako sem se vsega rokovanja z obema sistemoma naučil na podlagi dokumentacije, ki jo oba proizvajalca ponujata na spletu. Podjetje Oracle za svoj izdelek ponuja zelo obširno tehnično dokumentacijo, ki obsega namestitvena navodila za vse možne kombinacije podprtih okolij, rokovanje z obema administracijskima vmesnikoma in pa dokumentacijo za vsako verzijo izdanega konektorja. Microsoft je pri vsem skupaj zelo skop, nudijo nekaj vodičev za povezavo z različnimi sistemi, ki pa bralcu ne nudijo vsebinskega razumevanja celotnega sistema. Oba proizvajalca imata tudi spletno skupnost organizirano v obliki foruma, kjer sem izbrskal veliko koristnih informacij kako kaj nastaviti.

Glede na zelo zahtevno namestitev sistema OIM sem pričakoval, da bo takšno tudi njegovo upravljanje preko administracijskih vmesnikov. Vendar temu ni bilo tako. Oba administracijska vmesnika, s katerima upravljamo OIM sistem, imata zelo logično razporejena vsa opravila, ki jih administrator oziroma integrator potrebuje pri svojem delu. Ena izmed prednosti vmesnika ILM je odzivnost, kar je po svoje logično, saj gre za namizno aplikacijo in ne spletni vmesnik kot pri Oraclu. Hkrati je to tudi pomanjkljivost, saj spletni vmesnik omogoča upravljanje znotraj administrativne varnostne meje, ki jo določimo sami – ne da bi zato morali uporabljati razne »remote desktop« aplikacije. Administracijski vmesnik ILM-ja zgleda v primerjavi s konkurentom prav špartansko. To je po svoje zelo pozitivna lastnost. Podrobnejša analiza sistemov pokaže, da je to posledica veliko manjše podprtosti standardnih storitev oskrbovanja uporabnikov, saj ILM nima niti tako osnovnih funkcionalnosti, kot je vmesnik za samopostrežne funkcije oskrbovanja, kot je recimo ponastavitev gesla itn. Podpora manjšemu naboru funkcionalnosti standardnih storitev oskrbovanja pri implementaciji mojega testnega scenarija ni igrala nobene vloge, saj sem do tega dejstva dokopal že na podlagi opisa izdelkov iz »poglavja 5.« in temu je bil prilagojen tudi testni scenarij.

	Dokumentacija	Administracijski vmesnik	Funkcionalnost konektorjev
Oracle Identity Manager	9	8	10
Microsoft Identity Lifecycle Manager	6	7	6

Tabela 6.2: Primerjalna tabela izkušenj s sistemom na podlagi problemske domene

Najpomembnejša lastnost, ki olajša implementacijo sistemov v poslovno okolje, je vsekakor nabor funkcionalnosti vgrajenih konektorjev in prav na tej točki je ILM najbolj razočaral. Konektorji so namreč tako slabo prilagojeni za povezovanje z oddaljenimi viri, da je že za tako tipično operacijo, kot je ustvarjenje identitete v drugem sistemu, potrebno ročno poseči v postopek in sprogramirati kodo, ki manjka. Zelo nenavadna poteza Microsofta je, da podobne funkcionalnosti niso vgradili v sam sistem. Posebej ob podatku, da izid prej omenjenega orodja datira v leto 2004, medtem ko je bila trenutna verzija ILM sistema splavljena na trg v letu 2007.

Preslikovanje atributov me je tudi bolj navdušilo v sistemu OIM. Zelo ličen čarovnik namreč vse potrebno postori na bolj uporabniku prijazen način, kot ILM. Odpade namreč iskanje po dokumentaciji AD, kateri atribut ima kakšno ime v shemi AD - to velja seveda samo za tipične scenarije, kakor je bil moj. Ker je Oracle ubral pri tako imenovanih »že vgrajenih« konektorjih za povezavo z oddaljenimi sistemi pristop, da konektorji niso »fizično« vgrajeni v sistem. To seveda pomeni, da jih je treba namestiti ročno. S tem so uporabnike prisilili, da vedno uporabljajo najnovejše konektorje. Po drugi strani bi pa lahko postopek bil malo bolj avtomatiziran. Potrebno je namreč ročno kopiranje datotek in brisanje medpomnilnika strežnika, vse to bi se verjetno dalo izpeljati tudi preko administracijskega vmesnika. Pri uporabi sistema ILM me je zmotila tudi terminologija, ki jo uporablja Microsoft, ker deloma odstopa od standardne IDM terminologije. Potrebno je namreč podrobno poznati vse izraze, da lahko nastaviš ustrezne preslikave atributov in izvedeš usklajevanje.

Poglavje 7:

SKLEPNE UGOTOVITVE

Moje diplomsko delo je imelo več ciljev. V prvem sklopu sem želel na splošnem primeru pojasniti kaj je to upravljanje z digitalnimi identitetami. Ugotovil sem, da je to zelo kompleksno področje, ki ga le stežka stlačimo v neko ogrodje ali kalup, saj ga prepletajo številne tehnologije in koncepti iz različnih področij informacijske tehnologije. Pri tem sem imel težave z iskanjem ustrezne literature, saj zavoljo obširnosti področja obstaja zelo malo kvalitetnih virov, ki bi se celostno lotevali tematike.

En izmed ciljev drugega sklopa diplomskega dela je bil osvetliti poslovne koristi, ki jih prinese uporaba teh sistemov v praksi. Podal sem nekaj primerov kako lahko podjetja zmanjšajo stroške namenjene za informatiko, kakšne prednosti prinašajo končnim uporabnikom in kaj pomeni izboljšana varnost na ravni celotne organizacije. V nadaljevanju sem identificiral vodilna podjetja na področju sistemov za oskrbovanje uporabnikov, ta so: Oracle, IBM, Sun, Novell, CA in Courion. Vsa našteta razen zadnjega igrajo vodilno vlogo tudi na področju celovitih sistemov za upravljanje identitet, kamor bi lahko prišteli še segmente federacije, enotne prijave in upravljanja dostopov.

Z implementacijo scenarija problemske domene sem spoznal in tudi v praksi uporabil Oracle Identity Manager (OIM) ter Microsoft Identiy Lifecycle Manager (ILM). Želel sem ugotoviti ali je Microsoftov ILM res slabši od Oraclovega izdelka. Ocenjujem, da OIM potrjuje svoj status vodilnega sistema na področju oskrbovanja uporabnikov.

Microsoftovega sistema ILM ne prekaša le v podprtih storitvah in neodvisnosti od okolij, na katerih lahko deluje, temveč tudi pri povezovanju z identitetnimi viri, ki sem jih testiral. »Vgrajeni konektorji« OIM namreč podpirajo tipična administratorska opravila na način »out of the box«. To pomeni, da odpade potreba po programiranju, ki je pri ILM značilna tudi v zelo tipičnih scenarijih. Obširna

tehnična dokumentacija in spletna skupnost Oraclovega sistema nudita začetniku možnost hitrejšega reševanja težav pri implementaciji sistema v praksi.

Kljub zgoraj omenjenim dejstvom je tudi ILM dokaj soliden sistem. Potem, ko ga enkrat nastavimo svoje delo opravi enako dobro. ILM pa ima še enega asa v rokavu, ki morda prevesi tehtnico v primerjavi s konkurentom na njegovo stran. To je cena, ki ob dejstvu, da gre za zelo drage sisteme vsekakor ni zanemarljiv dejavnik. Microsoft je namreč pri stroških licenciranja in implementacije najcenejši med ponudniki teh izdelkov. ILM, ki povsem zadovolji osnovne potrebe pri oskrbovanju uporabnikov, ponujajo za 50% do 65% cene, ki jo zahtevajo vodilni konkurenti.

7.1. Pogled naprej

Prihodnost, predvsem leto 2010 bo zelo pestro na področju sistemov za upravljanja digitalnih identitet. Ključna igralca, na katera bo pozorna javnost, sta ravno izdelovalca sistemov, ki sem ju primerjal v svojem delu, torej Microsoft in Oracle.

Microsoft je že za leto 2008 napovedoval splavitev izdelka ILM 2, ki se bo preimenoval v Forefront Identity Manager. Izdelek do trenutka pisanja tega diplomskega dela še ni ugledal luči sveta in je najavljen za prvo četrtletje 2010. Nova, izboljšana verzija izdelka bo po napovedih Microsoftovih inženirjev končno resneje konkurirala vodilnim izdelkom na trgu IDMS. Nov rod izdelka naj bi ponudil tudi preprost vmesnik za samo-oskrbovanje in administriranje uporabnikov, obnovljena bo seveda tudi knjižnica vgrajenih konektorjev in pa odpravljene nekatere pomanjkljivosti, na katere sem opozoril tudi v svojem delu.

Drug ključni dogodek, pa se je zgodil poleti 2009 in bo lahko še kako zamajal IDM krajino. Oracle je s prevzemom Suna pridobil tudi njegov bogat portfelj IDM izdelkov, zato bo zelo zanimivo opazovati kako bo le-tega implementiral v svoj obstoječ portfelj ponudbe celovitih in parcialnih sistemov za upravljanje digitalnih identitet.

SEZNAM SLIK

SEZNAM TABEL

LITERATURA

[1] M. Bokal, "Vzpostavitev enotnega Aktivnega imenika na Univerzi v Ljubljani," 2008.

[2] Burton Group, "Oracle's Approach to Identity Management," 2005.

[3] Burton Group, "Provisioning Market 2009: Divide and Conquer," 15.1.2009.

[4] Gerald Carter, *LDAP System Administration*.: O'Reilly, 2003.

[5] H. Links Corbin, *IAM Success Tips, Volume 1*.: Links Business Group LLC, 2008.

[6] H. Links Corbin, *IAM Success Tips, Volume 2*.: Links Business Group LLC, 2008.

[7] Deloitte & Touche. (2009, Sep.) Identity Management Roadmap. Dostopno na: http://www.provost.utoronto.ca/public/reports/overview/appendices/a.htm

[8] Forrester Research, Inc., "The Forrester Wave: Identity And Access Management, Q1 2008," 2008.

[9] Gartner, Inc., "Magic Quadrant for Directory Servers, 2H03," 2003.

[10] Gartner, Inc., "Magic Quadrant For User Provisioning," 2009.

[11] HP. (2009, Oct.) The HP Security Handbook. Dostopno na: http://h71028.www7.hp.com/ERC/downloads/HP%20Security%20Handbook%20V2.pdf

[12] HP, Jan De Clercq, and Jason Rouault. (2009, Oct.) An Introduction to Identity Management. Dostopno na: http://iranmath.googlepages.com/idmgt_intro.pdf

[13] Laura E. Hunter and Robbie Allen, *Active Directory Cookbook, 3rd Edition*.: O'Reilly Media, Inc., 2008.

[14] IDC, "Worldwide Identity and Access Management 2008-2012 Forecast with Submarket Segments," 2008.

[15] Lianzhong Liu and Junxiu Gao, "An organization-oriented model for federated identity management and its application," in *6th IEEE International Conference on Industrial Informatics (INDIN)*, Daejeon, South Korea, 2008.

[16] Microsoft. (2009, Sep.) Microsoft Identity Lifecycle Manager 2007 FP1. Dostopno na: http://www.microsoft.com/windowsserver/ilm2007/

[17] R. Morimoto, M. Noel, O. Droubi, R. Mistry, and C. Amaris, *Windows Server 2008 Unleashed*.: Sams Publishing, 2008.

[18] Oracle. (2009, Sep.) Oracle Acquires Oblix. Dostopno na: http://www.oracle.com/corporate/press/2005_mar/oblix.html

[19] Oracle. (2009, Aug.) Oracle Identity Manager. Dostopno na: http://www.oracle.com/technology/products/id_mgmt/oxp/index.html

[20] Oracle. (2009, Aug.) Oracle Identity Manager Connectors Documentation. Dostopno na: http://download.oracle.com/docs/cd/E11223_01/index.htm

[21] Oracle. (2009, Aug.) Oracle Identity Manager Documentation. Dostopno na: http://download.oracle.com/docs/cd/E10391_01/index.htm

[22] Oracle, "Oracle Identity Manager, An Oracle White Paper," 2008.

[23] E. Perkins and P. Carpenter, "Magic Quadrant for User Provisioning," Gartner Research, 30.9.2009.

[24] Archie Reed, *The Definitive Guide To Identity Management*.: Realtimepublishers.com, 2004.

[25] Beth Sheresh and Doug Sheresh, *Understanding Directory Services*.: Systems Research Corporation, 2002.

[26] Slovar infromatike. islovar. Dostopno na: http://www.islovar.org

[27] J. Sodnik, *Preprost protokol za dostop do imenika LDAP*., 2002.

[28] The Radicati Group. (2009, Oct.) Reducing Costs and Improving Productivity with an Identity Management Suite. Dostopno na: Reducing Costs and Improving Productivity with an Identity

Management Suite

[29] Mark C. Smith, Gordon S. Good Timothy A. Howes Ph.D., *Understanding and Deploying LDAP Directory Services, Second Edition*.: Addison Wesley, 2003.

[30] K. Tracy, "Identity management systems," *IEEE Potentials*, vol. 27, no. 6, November-December 2008.

[31] Wikipedia. (2009, Oct.) Biometrija. Dostopno na: http://sl.wikipedia.org/wiki/Biometrija

[32] Wikipedia. (2009) Directory service. Dostopno na: http://en.wikipedia.org/wiki/Directory_server

[33] Wikipedia. (2009, Sep.) Identity Lifecycle Manager. Dostopno na: http://en.wikipedia.org/wiki/Identity_Lifecycle_Manager

[34] Wikipedia. (2009, Oct.) Identity management. Dostopno na: http://en.wikipedia.org/wiki/Identity_management

[35] Wikipedia. (2009, Oct.) Security token. Dostopno na: http://en.wikipedia.org/wiki/Security_token