

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

**IZBOR IN UVAJANJE SISTEMA ZA UPRAVLJANJE Z
IDENTITETAMI**

Ljubljana, april 2013

MATEVŽ KRISTAN

IZJAVA O AVTORSTVU

Spodaj podpisani **Matevž Kristan**, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor magistrskega dela z naslovom **IZBOR IN UVAJANJE SISTEMA ZA UPRAVLJANJE Z IDENTITETAMI**, pripravljenega v sodelovanju s svetovalcem **prof. dr. Alešom Groznikom**.

Izrecno izjavljam, da v skladu z določili Zakona o avtorski in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
 - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
 - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne _____

Podpis avtorja: _____

KAZALO

UVOD	1
1. UPRAVLJANJE IDENTITET	7
1.1 Opredelitev upravljanja identitet.....	7
1.1.1 Izzivi upravljanja identitet	9
1.1.2 Prednosti upravljanja identitet	11
1.1.3 Organizacijski in tehnični pristop k upravljanju identitet	14
1.1.4 Funkcionalnosti sistemov upravljanja identitet	15
1.1.4.1 Življenjski cikel računov	16
1.1.4.2 Upravljanje profilov	16
1.1.4.3 Delovni tok	16
1.1.4.4 Dodeljevanje pravic in razpuščanje	17
1.1.4.5 Delegirano upravljanje	18
1.1.4.6 Samopostrežba.....	19
1.1.4.7 Upravljanje gesel	19
1.1.4.8 Nadzor dostopa na podlagi vloge	20
1.1.4.9 Revizija in poročanje	21
1.1.5 Standardi na področju upravljanja identitet.....	22
1.2 Upravljanje identitet v Sloveniji	23
2. OKOLJE IN SISTEMI UPRAVLJANJA IDENTITET.....	27
2.1 Okolje, sistemi in potreba po upravljanju identitet	27
2.1.1 Okolje	28
2.1.2 Sistemi in storitve	29
2.2 Sistemi upravljanja identitet	34
2.2.1 Komponente sistemov upravljanja identitet	35
2.2.1.1 Imeniške storitve in imeniki	35
2.2.1.2 Življenjski cikel identitet	38
2.2.1.3 Varnostni mehanizmi in upravljanje dostopov ter overitev	39
2.2.1.4 Sistemi revizije in poročanja	41
2.2.2 Entitete sistemov upravljanja identitet	41
2.2.2.1 Identiteta	42
2.2.2.2 Sistem	42
2.2.2.3 Vloga	43
2.2.2.4 Dodeljevanje vlog.....	43
2.3 Predstavitev in analiza sistemov za upravljanje identitet.....	43
2.3.1 Dejavniki in karakteristike izbora sistemov	44
2.3.2 Vodilni ponudniki rešitev.....	45
2.3.2.1 Oracle (vključno s podjetjem Sun)	46
2.3.2.2 IBM Tivoli	47
2.3.2.3 Computer Associates (CA)	47
2.3.2.4 Novell	48
2.3.2.5 Courion	48

2.3.2.6	Microsoft in Omada	49
2.3.3	Izbor in ostali ponudniki	50
2.3.3.1	Pristop k analizi ponudb	51
3.	VPELJAVA SISTEMA UPRAVLJANJA IDENTITET V PODJETJE	56
3.1	Predstavitev podjetja Krka, d. d.	56
3.1.1	Sektor za informacijske tehnologije in telekomunikacije	57
3.1.2	Službi v SITT	58
3.2	Uporabniške zahteve za vpeljavo sistema upravljanja identitet.....	59
3.2.1	Predstavitev trenutnega stanja	59
3.2.2	Opis trenutnega stanja aktivnega imenika.....	60
3.2.3	Zahteve delovanja sistema	62
3.2.3.1	Opis funkcionalnosti	62
3.2.3.2	Načini delovanja.....	71
3.2.3.3	Napake in akcije ob možnih napakah.....	71
3.2.3.4	Varnost in zaščita zahtevana na sistemu.....	71
3.2.4	Podatki, zapisi ter podpisi v sistemu	71
3.2.4.1	Podatki.....	72
3.2.4.2	Zapisi	73
3.2.4.3	Podpisi.....	73
3.2.4.4	Vmesniki	73
3.2.4.5	Okolje in varnost delovanja sistema.....	74
3.2.4.6	Sistem avtorizacij (postopki).....	75
3.2.4.7	Omejitve sistema	75
3.2.4.8	Dokumentacija sistema	75
3.3	Možnosti in strategija vpeljave sistema upravljanja identitet	76
3.3.1	Metodologija ITIL.....	76
3.3.2	Dobra proizvodna praksa (GMP) v farmacevtski industriji	79
3.3.3	FDA predpisi	80
3.4	Postopek vpeljave izbrane rešitve	81
3.4.1	Vzpostavitev projekta.....	82
3.4.2	Projektna skupina	82
3.4.3	Priprava na izvedbo projekta.....	83
3.4.4	Priprava uporabniških zahtev	84
3.4.5	Izbira dobavitelja.....	84
3.4.6	Priprava funkcionalne in dizajn specifikacije	85
3.4.7	Izvedba projekta	85
3.4.8	Namestitev in testiranje.....	86
3.4.9	Primopredaja sistema	87
3.4.10	Uporaba sistema	88
3.4.11	Opredelitev odgovornosti med izvajanjem projekta	88
3.4.12	Dokumentacija za potrditev kontrol izvajanja postopka	89
3.4.13	Izvedba kvalifikacije sistema upravljanja identitet	89
3.4.14	Ključni elementi sistema upravljanja infrastrukture	90
3.5	Postopek kvalifikacije sistema.....	93
3.5.1	Življenjski cikel kvalifikacije sistema.....	95

3.5.2 Dokumentacija kvalifikacije sistema.....	95
3.6 Ocena posledic vpeljave upravljanja identitet.....	99
SKLEP	103
LITERATURA IN VIRI.....	106

KAZALO SLIK

Slika 1: Identitete in okvir identitet	10
Slika 2: Tipična umestitev sistemov IdM in povezava na druge sisteme	29
Slika 3: Aktivni imenik in atributi uporabniškega računa	31
Slika 4: Urejanje skupin v AD.....	32
Slika 5: Shema umestitve IdM sistema.....	34
Slika 6: Primer meta-imenika in virtualnega imenika	37
Slika 7: Življenjski cikel identitete.....	38
Slika 8: Prijavno okno: uporabnik, geslo, domena (levo), na desni brez domene.....	40
Slika 9: Entitete	42
Slika 10: Vodilni ponudniki IdM rešitev 2010 in 2011	46
Slika 11: Vmesnik Omada	55
Slika 12: Služba informatike v Krki	58
Slika 13: Notranji aktivni imenik	61
Slika 14: Zunanji aktivni imenik	61
Slika 15: Izstop	64
Slika 16: Dodatni naslov elektronske pošte.....	65
Slika 17: Sprememba podatkov	67
Slika 18: Upravljanje posebnih računalniških računov	68
Slika 19: Dodajanje računalnika v aktivni imenik.....	69
Slika 20: Upravljanje s skupinami.....	70
Slika 21: Povezava FIM, OIM in ostalih sistemov.....	74
Slika 22 : Okvir zbirke ITIL	78
Slika 23: Postopek odobritve IT projekta na nivoju Krke	83
Slika 24: Shema postopka.....	87
Slika 25: Horizontalni pristop kvalifikacij	90
Slika 26: Izdelava plana kvalifikacij	93
Slika 27: Življenjski cikel kvalifikacije sistema – V model	95

KAZALO TABEL

Tabela 1: Število podjetij v Sloveniji, po velikosti, 2000-2005	24
Tabela 2: Dodeljevanje vlog in tipi.....	43
Tabela 3: Tabela kriterijev, uteži in ocen ponudnikov	54
Tabela 4: Tabela ustreznosti ponudnikov glede na uporabniške zahteve	54
Tabela 5: Tabela vlog v sistemu.....	74
Tabela 6: Odgovornosti pri projektu.....	88
Tabela 7: Obseg kvalifikacij	91
Tabela 8: Določevanje dodatnih aktivnosti na osnovi postopka.....	94

UVOD

Opis problematike. Večina podjetij danes, tako velikih kot majhnih, uporablja več različnih sistemov pri upravljanju, nadzoru in izvajanju nalog in opravil v svojem poslovanju. Pogost problem, ki je opazen zlasti v velikih podjetjih, leži v obvladovanju raznih dostopov, pravic, nalog ipd. posameznika, ki se giblje skozi delovni proces, v kontroli teh dostopov in pravic ter ne nazadnje sledljivosti sprememb v dostopih in pravicah posameznikov. Najbolj pomembni sistemi glede samega namena podjetja in nalog posameznikov in skupin v podjetju izvirajo iz kadrovskih sistemov, saj je vsak zaposleni najprej naveden v kadrovski evidenci, v kateri že dobi določene opisne attribute, kot na primer v kateri službi je zaposlen, na katerem delovnem mestu in posledično je iz kadrovske strukture razvidno tudi komu je odgovoren za svoje delo. Naknadno se v obliki elektronske pošte oziroma formuliranega pisemskega ali elektronskega obrazca zahteve pošljejo raznim oddelkom za dodelitev raznih dostopov do delov sistema, ki ga zaposleni potrebuje za svoje delo. Najbolj tipični sistemi v podjetju so **elektronska pošta** (dodelitev elektronskega poštnega naslova novo zaposlenim), **datotečne storitve** (dodelitev dostopov do skupnih oddelčnih vsebin, ki pripadajo delovnemu mestu zaposlenega), **Intranet storitve** (zelo podoben sistem dodeljevanja pravic kot datotečnih storitev), **poslovne aplikacije** (dostopi do posameznih funkcionalnih delov sistema), **proizvodne aplikacije** (oziroma aplikacije za nadzor proizvodnje, ki so lahko tudi del poslovnih aplikacij) itd. Na tem mestu bi še posebej izpostavil **imeniške storitve** (angl. *Directory Services*) oziroma poznane tudi kot aktivni imenik (angl. *Active Directory*) – ki je posebna baza podatkov o uporabnikih, njihovih prijavah, osebnih podatkih, podatkih o IT objektih (na primer osebni računalniki, strežniki, skupine itd.). Poleg kadrovske baze, ki je **primarni izvor** vseh podatkov o zaposlenih, ji tesno sledi aktivni imenik, ki del podatkov črpa direktno iz kadrovske baze, del pa pridobi skozi ostale sisteme in direktno skozi interakcijo skrbnika aktivnega imenika.

Če se torej na kratko vrnemo k majhnim podjetjem, kjer večino informacijskih storitev obvladuje en sam skrbnik oziroma manjša skupina skrbnikov, se zahtevane spremembe na več sistemih izvajajo relativno dosledno in ažurno, medtem ko se v večjih podjetjih zaradi obilice zahtevkov in počasnih protokolov (na primer papirna oblika zahtevkov) pojavljajo čedalje daljše čakalne vrste pri realizaciji zahtevkov in posledično upada storilnost, saj kadrovske spremembe ne omogočajo istočasno tudi uporabe novih virov in delovnih okolij. Sam nadzor in sledljivost nad izvedenimi spremembami pa se v primeru majhnega ali velikega podjetja hitro izgubi brez systemskega, elektronskega vodenja in izvajanja sprememb.

Predvsem velika mednarodna podjetja, ki imajo centralne informacijske sisteme vodene iz centralne lokacije (kot je tudi pogosta praksa v takih podjetjih), v svoji kompleksnosti

izgubljajo nadzor in sledljivost nad različnimi dostopi in pravicami zaposlenih. Izrazit primer nedoslednosti so prehodi zaposlenega iz enega delovnega mesta na drugo. Ker zaposleni pogosto še nekaj časa bodisi zaključuje naloge iz prejšnjega delovnega mesta ali pomaga novemu kadru na svojem starem delovnem mestu, začasno še potrebuje prejšnje pravice. V naslednjih mesecih skrbniki navadno pozabijo na opravilo odstranitve pravic (kar je redko posebej opredeljeno) in če sistem tega ne stori sam, tako tudi ostane. Potreba po centralnem nadzoru in avtomatiziranem dodeljevanju pravic in dostopov s pravo mero sledljivosti spremembam je torej skorajda nujna oziroma potreba po tem je večja proporcionalno z velikostjo podjetja.

Na trgu se danes že pojavljajo tudi orodja, ki omogočajo upravljanje identitet na obstoječih sistemih v podjetju. Sistemi upravljanja identitet se danes pojavljajo pod skupno kratico in imenom (v nadaljevanju) **IdM Sistemi** (angl. *Identity Management Systems*). Eden izmed ciljev naloge je tudi predstavitev izbire enega izmed sistemov ter implementacija sistema kot orodja v delovno okolje podjetja Krka, d. d., z razdrobljenim poslovanjem po celem svetu.

Če torej v grobem povzamem, kaj za nas pomeni sistem upravljanja identitet v nalogi, gre za naslednje:

- sistem, katerega uporabniki izvirajo iz avtoritativnega vira (na primer kadrovske evidence) ter se kreacija identitete ter tudi skrb za to identiteto vodi prav v tem sistemu;
- sistem, ki zagotavlja, da je identiteta enovita ter neoporečna – torej preverja pristnost identitete redno in jo ščiti proti zlorabam in neavtoriziranim spremembam;
- sistem, ki omogoča uporabo teh identitet v procesih *avtentikacije* (preverjanja pristnosti) in avtorizacije v realnem času s primerno stopnjo varnosti.

Predmet preučevanja je torej način in možnost upravljanja identitet v velikih podjetjih, ki ga bom prikazal na primeru farmacevtskega podjetja Krka, d. d., iz Novega mesta. Potrebno je poudariti, da se je smiselno ukvarjati z upravljanjem identitet predvsem v velikih podjetjih, saj sami stroški vpeljave takih sistemov običajno presegajo zmožnosti majhnih podjetij, po drugi strani pa manjša podjetja niso tako podvržena težavam, ki sem jih omenjal v uvodu, saj je kompleksnost njihovega poslovanja in število zaposlenih bistveno manjše in lažje obvladljivo. Glavni cilj vpeljave IdM sistema je znižati stroške poslovanja, razbremeniti zaposlene z avtomatskim izvajanjem procesov, povečati stopnjo zaupnosti delegiranih pravic, izločiti človeške napake v procesu, izboljšati nadzor in sledljivost nad spremembami – kar bodo tudi delni cilji same naloge.

Opredelitev namena in ciljev. Temeljni cilj magistrskega dela je raziskati in analizirati rešitve za izvajanje in upravljanje identitet ter identificirati možnosti vpeljave sistema za

upravljanja identitet v velikem podjetju. Za doseg temeljnega cilja je potrebno zajeti širši pogled na področje upravljanja identitet, zato iz temeljnega cilja izhajajo naslednji pomožni cilji.

Da bi ugotovili, kakšne možnosti vpeljave upravljanja identitet v svoje poslovanje ima neko podjetje, je potrebno najprej jasno opredeliti pojem upravljanja identitet (prvi pomožni cilj). Nadalje je potrebno opredeliti in analizirati okolje upravljanja identitet ter ponudbo sistemov za upravljanje identitet (drugi pomožni cilj). Nato je potrebno izbrati in analizirati nekaj primernih rešitev za upravljanja identitet (tretji pomožni cilj). Četrty pomožni cilj pa se nanaša na oblikovanje strategije vpeljave sistema za upravljanja identitet v izbranem podjetju ter oceno posledic tega dejanja z vpeljavo izbrane rešitve v tretjem pomožnem cilju. Navedeni pomožni cilji omogočajo uresničitev temeljnega cilja magistrskega dela.

Področje upravljanja identitet kot predmet preučevanja sem izbral predvsem iz razloga poznavanja problematike pri upravljanju več različnih računalniških sistemov v podjetju Krka, kjer delam kot sistemski skrbnik in vodja projektov v službi informacijskih tehnologij in telekomunikacij že od leta 2003. Moje primarno področje dela na začetku kariere je bilo področje internetnih strani in intraneta, kjer sem se pri slednjem srečal s težavo obvladovanja uporabniških dostopov od posameznih segmentov vsebin intraneta do povezovanja pravic dostopov med intranetom in datotečnimi storitvami, za katere je bil določen drug skrbnik in je usklajevanje nalog zahtevalo dodatne aktivnosti. Kljub vpeljavi domenskih skupin, ki so uporabnike združevale po oddelkih in službah, za poenostavitev upravljanja uporabniških dostopov, so še vedno ostajale aktivnosti, za katere smo morali skrbeti skrbniki sistemov sami in v lastni organizaciji (na primer uporaba elektronskih opozoril, kdaj je potrebno izvesti kakšno spremembo).

Prvotno smo upravljanje identitet reševali tudi z manjšimi namenskimi programi za posamezne sisteme, ki so zelo pripomogli k obvladovanju predvsem časovno zamaknjenih opravil ter omogočali sledljivost izvedenim spremembam. Šele konec leta 2009 se je vodstvo službe odločilo o celovitem pristopu k upravljanju identitet in sam sem imel tudi priložnost sodelovati na projektu kot eden izmed skrbnikov sistemov. V nalogi bom opisal, kako smo izbrali in vpeljali rešitev v podjetje Krka, d. d., ter kakšne prednosti in slabosti je vpeljava prinesla.

S pomočjo prej zastavljenih ciljev si lahko raziskovalno vprašanje določim z namenom iskanja čim boljšega odgovora, kako in katero orodje vpeljati, da bodo izhodiščne uporabniške zahteve izpolnjene v čim večji meri. Odgovor na to vprašanje bo naloga sama, ki v celoti služi kot vodič za vsakršno razmišljanje o vpeljavi sistema upravljanja identitet v podjetje. Naloga ni ne izrazito tehnično ne procesno usmerjena, je pa osredotočena na prikaz metod in postopkov, ki jih narekujejo standardi in dobre poslovne prakse pri

vpeljavi kompleksnih sistemov, ki vplivajo na same infrastrukturne elemente v podjetju in na prenovo osnovnih procesov.

Opredelitev metode dela. V magistrski nalogi se bom posluževal več raziskovalnih pristopov oziroma metod preučevanja, ki se v grobem delijo po zastavljenih ciljih oziroma pomožnih ciljih, ki sem jih opisal v prejšnji točki.

V uvodnem teoretičnem delu si bom pomagal najprej s splošno raziskovalno metodo spoznavnega procesa, kjer bom pridobil podatke iz že objavljenih strokovnih del s področja upravljanja identitet ter ostala pomembna dejstva in informacije s preučevanega področja. Te podatke bom nato obdelal še z metodo opisovanja ter tudi opredelil temeljne pojme, ki so pomembni za nadaljevanje študije upravljanja identitet. Vse tako pridobljene podatke bom skozi metodo analize podatkov primerno obdelal ter tako predstavil ugotovitve in izhodišča za izvedbo študije primera. Torej bom z metodo opisovanja opisoval dejstva, procese in pojave, ki nastopajo v raziskovalnem okolju. Poleg opisovanja in analize pa si bom pomagal še z metodo kompilacije (povzetek stanj procesov in opazovanj posameznih pojavov ter tudi primerjavo rezultatov s stališči nekaterih avtorjev iz literature).

V praktičnem bo magistrska naloga obsegala študijo primera vpeljave sistema upravljanja identitet v podjetje, zato lahko na začetku ugotovimo, da bo sama raziskovalna naloga temeljila predvsem na deduktivnem pristopu, kot deloma tudi na induktivnem pristopu, kar je pogosto značilno za analizo kvalitativnih podatkov v študijah primerov. Praktični primer bo slonel na primerih uporabe sistemov za upravljanje po svetu in doma, ki bodo podali z metodo analize sekundarnih podatkov smernice (oziroma prednosti in slabosti) kateri sistem je najbolj primeren glede na uporabniške zahteve in lastnosti okolja, v katerega se sistem vpeljuje.

Glede deduktivnega pristopa lahko povemo, da že obstajajo teorije, kako sistemi upravljanja identitet poenostavijo upravljanje identitet celostno ter tudi vzpostavijo sledljivost spremembam ter povečujejo pregled nad pravicami posameznikov ter zmanjšujejo verjetnost zlorabe pravic, ki se ne odstranjujejo dovolj ažurno. Induktivni pristop h končnemu rezultatu pa se bo kazal kot oblikovanje sklepa oziroma teoretične predpostavke, katero izmed orodij ali načinov vpeljave sistema za upravljanje identitet je najbolj primerno v danih pogojih.

Zbiranje primarnih podatkov v okviru študije primera pa bom opravil z več tehnikami: analizo internih dokumentov (uporabniške zahteve, načrt rešitve, tehnična specifikacija rešitve...), preučevanjem nekaterih posameznikov, ki se jih nov način dela preko sistema IdM pogosto dotika, lastne izkušnje pri uporabi sistema in nekatere posledice v izvedbi nalog s pomočjo novega sistema. V splošnem bom iz sekundarnih podatkov, vzetih kot

osnova za nadaljnjo obdelavo, oblikoval rezultate, ki bodo služili kot primarni podatki v nadaljnjih obdelavah.

Skozi celotno nalogo se bom opiral tako na ugotovitve domače kot tudi tuje strokovne literature in ostalih dostopnih virov (splet, standardi, viri, članki, prispevki ipd.), ki teoretično in praktično obravnavajo področje upravljanja identitet. V pomoč pri pripravi dela mi bodo tudi pridobljene praktične izkušnje, saj sem že 10 let zaposlen kot sistemski inženir in se s problematiko pravic in dolžnosti uporabnikov dnevno srečujem pri svojem delu.

Problematika zbiranja in analize podatkov. Skozi cilje magistrske naloge si bom postavljaj raziskovalna vprašanja z namenom iskanja čim boljšega odgovora, kako in katero orodje vpeljati, da bodo izhodiščne uporabniške zahteve izpolnjene v čim večji meri. V tretjem poglavju dispozicije sem podal hipotezo, ki pa jo lahko razčlenimo tudi na vrsto podtrditvev, ki jih bom poskušal pokazati skozi nalogo. Torej je sama naloga še vedno predvsem usmerjena v iskanje odgovorov na ta vprašanja (oziroma te trditve).

Samo področje upravljanja identitet je, tako v svetu kot pri nas, še vedno relativno novo področje. Strokovne literature v obliki knjig je malo, obstaja pa veliko krajših člankov in prispevkov na internetu, ki zajemajo bodisi povzetke študij primerov ali pa splošne teoretične paradigme o upravljanju identitet. Same podatke o sistemih, ki so že ponujeni na trgu, bom pridobil relativno enostavno – iz dokumentacije proizvajalca in iz raznih člankov objavljenih na spletu. Sami podatki o sistemih v podjetju so prav tako na voljo v podobni obliki, vključil pa bom še primerjalne članke, saj so sistemi praviloma zreli in dobro dokumentirani ter predmet več preučevanj (zgolj zreli sistemi so primerni za povezovanje, kot bom ugotovil v nalogi).

S tako pridobljenimi podatki (vsi ti podatki so torej sekundarni) bom lahko odgovoril na prvi zastavljen pomožni cilj – torej jasno opredeliti pojem identitete in samega upravljanja identitete. Kot prvo spremenljivko bom torej opazoval spisek in število pod-sistemov, ki jih želimo povezovati v sistem za upravljanje identitet – seznam pod-sistemov bom tudi uredil od pomembnejšega do manj pomembnega za samo delovanje podjetja, ter tako določil osnovni minimalni nabor sistemov, potrebnih za izvedbo sistema upravljanja identitet. Na ta način bom pridobil podatke, s katerimi bom lahko sledil drugemu pomožnemu cilju, torej identifikaciji okolja, v katerem bom lahko kvalitetno izvedel nadaljnjo raziskavo izbire ustreznega sistema.

Ker sistemi v podjetjih nikakor niso vedno enaki, pa vendarle imajo neke skupne točke – problematika identifikacije teh skupnih sistemov iz nabora osnovnih sistemov predstavlja vmesni izziv za pridobitev realne splošne slike o tipičnih osnovnih sistemih v podjetjih.

Podatke bom pridobival ločeno za slovenska podjetja in tuja podjetja. Večino podatkov bom črpal iz opisov in predstavitev podjetij ter nekaj preko poznanstev (delo s partnerji ipd.) V največji meri predstavlja težavo zbiranja podatkov dejstvo, da so podjetja v zasebni lasti in ne objavljajo vseh podatkov o svojih sistemih – oziroma jih objavljajo nekonsistentno.

Največ podatkov bo na voljo za same ponujene rešitve na trgu, torej za izdelke, ki ponujajo celostno povezovanje sistemov. Zopet bom te sisteme vzorčil namerno, saj je eden izmed glavnih pogojev sprejetja določene rešitve kot prave prav pogoj, da zajema sisteme, ki jih želimo povezati – v kolikor ključnega sistema v naboru ni, potem je nesmiselno primerjati tak sistem. Podatke bom pridobil iz interneta oziroma iz spletnih strani proizvajalcev teh rešitev, ključne spremenljivke pa bodo prav posamezni sistemi in dejstvo, v kakšni meri izbrana rešitev rešuje povezljivost takega sistema.

Zadnji pomožni cilj v nalogi je oblikovanje strategije vpeljave sistema. Tu si bom pomagal predvsem z zbranimi primarnimi podatki, torej intervju z vodstvom in opazovanjem zaposlenih, deloma pa tudi s sekundarnimi podatki, ki jih bom zbral predvsem subjektivno preko spleta.

Zbrane podatke bom s pomočjo vrednotenja in povezovanja med seboj uredil in povezal s posameznimi pomožnimi cilji ter tako tudi odgovoril na podvprašanja, ki jih cilji zastavljajo. Skozi uresničitev štirih pomožnih ciljev bom torej oblikoval strategijo vpeljave sistema upravljanja identitet v velika podjetja.

Sama raziskava temelji v večini na deduktivnem pristopu. Za analizo kvalitativnih podatkov bom predvsem uporabil metodo oblikovanja razlag, saj bom predstavljene podatke analiziral v večini skozi razlago. Metodo induktivnega pristopa (prikaz in analiza podatkov) pa bom uporabil za oblikovanje strategije vpeljave sistema upravljanja identitet v velikih podjetjih. Tu se bom oprl predvsem na povzetke intervjujev in opazovanj. Prednost te metode je tudi kompatibilnost z metodami, temelječimi na deduktivnem pristopu, kar sovпада kombiniranim pristopom.

Znanstveni prispevek. Kot sem omenil v uvodu, je področje upravljanja identitet (predvsem celostno) relativno novo področje informatike, ki je nastalo iz potreb po preglednem upravljanju posameznikovih pravic in dostopov na raznih sistemih v podjetju, ki so nepregledni kot posledica mnogih razdrobljenih sistemov, kjer vsak opravlja neko ključno nalogo v podjetju.

V magistrski nalogi se bom lotil pristopa k upravljanju identitet celostno ter tako analiziral trenutne ključne sisteme, ki se pogosto uporabljajo v večjih podjetjih ter načine

povezovanja med njimi. Na trgu že obstajajo izdelki, ki omogočajo takšno ali drugačno obliko povezovanja sistemov med seboj, ključno pa je identificirati bazične sisteme in kako le-te najprimerneje celostno obvladovati skozi en vmesnik – izdelek. V samo študijo bom vključil tako pregled stanja, seznam sistemov, produkte – rešitve, ki že obstajajo ter tudi lastno analizo prednosti in slabosti posameznih rešitev, kot tudi načinov (tipov) povezovanja identificiranih ključnih sistemov.

Magistrska naloga v celoti pa bo tudi služila kot vodič oziroma izhodišče za kakršnokoli razmišljanje o vpeljavi sistema za upravljanje identitet v delovno okolje vsakega bralca, ki ga takšno področje in vpeljava takih sistemov oziroma povezovanje raznovrstnih sistemov kot takih tudi zanima.

1. UPRAVLJANJE IDENTITET

Kot bomo spoznali skozi nalogo, samo upravljanje identitet ni novo odkritje v svetu informatike, saj je večina sistemov, ki se uporabljajo danes, že vsebovala orodja in mehanizme nad uporabniki in njihovimi vlogami v tem določenem sistemu. V uvodu sem že omenil, da smo tudi v našem podjetju že uporabljali manjše namenske rešitve za posamezne sisteme. Nekateri izmed proizvajalcev sistemov so celo imeli več sistemov v svoji paleti izdelkov, katerih večkrat omenjena prednost je bila ravno »povezljivost« z ostalimi sistemi istega proizvajalca. Vsekakor je bila to konkurenčna prednost. Če danes pogledamo kot primer podjetje Microsoft, ki ponuja celo paleto izdelkov in sistemov, ki se tako ali drugače povezujejo med seboj in v veliki meri tudi omogočajo določena upravljanja sistemov skozi druge sisteme (kot primer lahko vzamemo Windows domeno in aktivni imenik, kjer ima skrbnik aktivnega imenika hkrati tudi dostop do vseh računalnikov v domeni, kot njihov skrbnik), bi lahko rekli, da je potreba po še večji povezljivosti sistemov izven obsega enega proizvajalca, nujna ob uporabi več sistemov.

Za boljše razumevanje upravljanja identitet (angl. *Identity Management*) si moramo najprej ogledati nekaj osnovnih definicij pojmov upravljanja identitet.

1.1 Opredelitev upravljanja identitet

Bistvo upravljanja identitet kot rešitve je v tem, da ponudi kombinacijo procesov in tehnoloških prijemov, ki omogočajo varno upravljanje dostopov do različnih virov in informacij (storitev) v podjetju, hkrati pa varuje osebne in zaupne podatke uporabnikov. Sistem upravljanja identitet zagotavlja možnost upravljanja takih procesov tako zunaj kot znotraj organizacije, torej za zaposlene, stranke, partnerje itd. (Reed, 2002, str. 1, 2).

Za boljše razumevanje pojmov naj povem, da se je skozi razvoj sistemov za upravljanje identitet pojavilo tudi veliko kratic, ki predstavljajo upravljanje identitet (angl. *Identity Management*), kot so IM, IdM, IDM, IMS itd. V nalogi bom uporabljal kratico IdM ali oznako IdM sistemi ali kar celotno ime »sistemi upravljanja identitet«.

V tem okviru lahko tudi IdM sisteme obravnavamo predvsem kot orodje, ki:

- definira entiteto (osebo, prostor, stvar),
- definira attribute entitet in jih hrani (ime, priimek, lokacija, naziv itd.),
- distribuira potrebne informacije skozi vnaprej pripravljene vmesnike,
- omogoča infrastrukturo za distribuiran način upravljanja identitet,
- skrbi za konsolidirano upravljanje relacij med entitetami po vnaprej definiranih pravilih.

Entitetam pogosto pravimo kar »objekti«, ki so običajno shranjeni v nekakšni bazi podatkov, ki ji pravimo tudi *Identity management store*. Pogosta oblika podatkovne baze za IdM sisteme je aktivni imenik (angl. *Active Directory*), ki temelji na LDAP¹ protokolu (kar bom še podrobneje opisal v nadaljevanju naloge). Aktivni imenik je strukturirana baza podatkov, ki je zasnovana tako, da hrani podatke o objektih ter tudi relacije med objekti. Hkrati pa ponuja že vgrajene metode za branje, urejanje, iskanje in posodabljanje obstoječih objektov (entitet).

Da bi lahko govorili o celostnem oziroma pravem upravljanju identitet znotraj podjetja, mora le-to zajemati tudi »objekte« izven podjetja – torej partnerje, dobavitelje, kupce kot tudi relacije med njimi in podjetjem samim. Če sistem upravljanja identitet zajema oba aspekta (notranjega in zunanjega), lahko govorimo o celostnem upravljanju identitet. Tako upravljanje identitet pa po drugi strani zahteva tudi prilagojeno infrastrukturo, saj naj bi torej sistem omogočal upravljanje bodisi iz intraneta, ekstraneta ali celo interneta. Za kar pa je potrebno vpeljati (če še niso) razne dostope do omrežja – neposredno ali preko navideznih privatnih omrežij (ang. *Virtual Private Networks*, v nadaljevanju VPN), z brezžičnimi dostopi itd. Torej je proces upravljanja identitet zakoreninjen že v **infrastrukturi** podjetja, ki jo je pogosto potrebno prilagoditi, če želimo uspešno vpeljati sistem upravljanja identitet.

Velikokrat se pri definiciji identitete uporablja izraz »digitalna identiteta«, ki predstavlja elektronsko hrambo podatkov o entitetah. Ti podatki so odvisni od nekaj dejavnikov: kdo je entiteta, okvir entitete (angl. *context*), profil entitete. Ker je digitalna identiteta pogosto odvisna predvsem od »**okvira**«, ki definira interakcijo entitete z digitalnim svetom podjetja

1 LDAP je kratica za Lightweight Directory Access Protocol

kot uporabnik, kupec, dobavitelj itd., po drugi strani pa je tudi odvisna od **profila** entitete, ki pa pove kakšna orodja, nastavitve in vire potrebuje entiteta za svoje delo – torej izvajanje vlog, ki jih povezuje okvir.

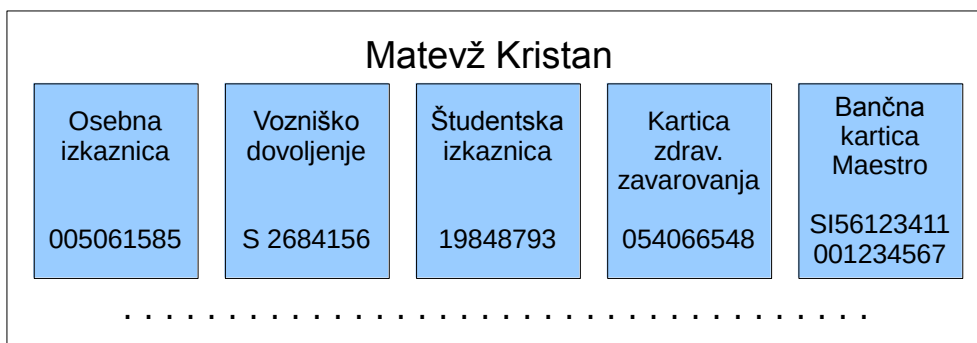
1.1.1 Izzivi upravljanja identitet

Zelo pomemben dejavnik pri uvajanju sistema upravljanja identitet je **centralizacija upravljanja**, ki na prvem mestu izpostavlja vprašanje varnosti. Tako varnosti pred zlonamernim dostopom do sistema ali napadom na sistem, kot tudi varnosti v smislu pravilne in prave uporabe sistema upravljanja identitet. Poleg tega pa se pojavijo tudi vprašanja pravilnosti uporabe identitete v določenem okviru. Na primer, če uporabimo pravo identiteto na nepravem mestu, kot to predvideva okvir identitete. Še posebno pozornost je potrebno usmeriti v preprečevanje uporabe prave identitete v pravem okviru, vendar jo uporablja napačna oseba (uporaba gesla sodelavca) itd. In veliko je še pomislekov predvsem v pravilnosti in varnosti uporabe sistema za upravljanje identitet, zato je pomembno izhodišče pri vpeljevanju sistema upravljanja identitet, da sistem **zagotavlja uporabo pravega okvira ob pravem času**.

Pri upravljanju identitet se moramo tudi zavedati, da vedno govorimo o **množici identitet** posameznika (slika 1). Izbran posameznik v podjetju ima svojo matično številko, naziv, elektronski naslov, telefonsko številko itd. kar vse predstavlja isto osebo – torej ima ena oseba (entiteta) več identitet. Kot sem omenil v prejšnjem odstavku, identitete povezuje in jim določa namen sam **okvir identitete**, torej tudi predvideva način uporabe in potrebna orodja ter tudi relacije med posameznimi identitetami. Okvir identitete je pomemben koncept, ki ga bom v nadaljevanju še večkrat omenil (Reed, 2002, str. 4).

Najširši način upravljanja identitet bi bil v globalnem smislu, torej mednarodno, medpodjetno itd., kjer bi vsaka oseba imela zelo veliko različnih identitet – če samo pomislimo koliko različnih identitet uporablja povprečen posameznik danes (osebna izkaznica, vozniško dovoljenje, plačilne kartice, članske kartice, prijave na različne spletne storitve ipd.), poleg tega pa bi jim morali definirati še okvir identitete, torej relacije med njimi. Poleg same obsežnosti in kompleksnosti podatkov posamezne entitete pa nastopi še vprašanje dostopnosti do podatkov. Obstaja veliko zaupnih podatkov, ki se ne delijo izven državnih organov, izven podjetij itd. V praktičnem pogledu se zdi tak način upravljanja nemogoč, medtem ko je znotraj zaključenih celot – na primer podjetij, upravljanje identitet zelo smiselni pristop, saj poenostavi uporabo predvsem za uporabnike in hkrati skrbi, da se procesi odvijajo po vnaprej določenih pravilih, kar ob sami pravilnosti le-teh zagotavlja tudi pravilno izvajanje. Ne nazadnje pa bi dovršen sistem upravljanja identitet v vseh podjetjih omogočil lažje razmišljanje o nadaljnjem globalnem upravljanju identitet, ki je bilo omenjeno prej.

Slika 1: Identitete in okvir identitet



Pri korporativnem upravljanju identitet, torej znotraj enega ali več podjetij, je predvsem značilno, da se uporabniki (zaposleni) identificirajo vedno na nek ustaljen način. Lahko se sicer identificirajo različno, na primer različno uporabniško ime za delo v programu SAP in različno uporabniško ime za prijavo v osebni računalnik, vendar mora tako za eno kot drugo storitev uporabiti določeno identiteto. Po drugi strani pa, ko uporabnik brska po internetu, želi večino informacij brskati kot anonimnež. Anonimnost je torej tudi okvir identitete, ki je uporabna predvsem v določenih primerih, ko uporabnik ne želi razkriti kdo je. Če se na kratko vrnemo k spletnem brskanju, torej brskamo po neki spletni trgovini anonimno, vse dokler se ne odločimo za nakup – potem pa je potrebno vnesti svoje podatke (običajno se ustvari račun z uporabniškim imenom in geslom, ki se poveže skupaj s podatki o uporabniku). To je pogosto v praksi danes, zasledimo pa občasno tudi vsebino, po kateri brez vzpostavitve identitete (torej anonimno) ne moremo brskati (dober primer je Krkina spletna stran s podatki o Krkinih zdravilih ali za zdravnike, ki zahteva prijavo za brskanje). V primeru sem nalašč navedel Krkino spletno stran zato, ker Krka, tovarna zdravil, d.d. (v nadaljevanju Krka) skozi svoj CRM (angl. *Customer Relationship Management*) določi uporabniška imena in osnovna gesla za zdravnike in farmacevte, s katerimi sodeluje. Torej bi lahko rekli, da so uporabniki v takem sistemu primarni, saj je njihova identiteta vzpostavljena iz **avtoritativnega vira** (Krkine baze strank in dobaviteljev – v pogostih primerih drugi spletni strani, kjer je možno uporabniški račun in geslo ustvariti samostojno, vnos podatkov je prepuščen uporabniku samem, je pa tudi zelo pogosta praksa, da uporabniki **ne vnašajo** pravih podatkov, saj ob prvem stiku sami ne vejo komu zaupajo podatke. Ta primer jasno opozarja tudi na vprašanja zaupnosti, zasebnosti in anonimnosti v vsakdanji rabi. Iz prakse je razvidno, da v kolikor nimamo možnosti »anonimnosti« potem bodo uporabniki ustvarili »lažno« identiteto, pod katero se počutijo anonimni. Koncepte zaupanja, zasebnosti in anonimnosti bom razložil podrobneje še v nadaljevanju.

Upravljanje identitet mora zagotoviti kreacijo identitete iz avtoritativnega vira, jo nato tudi upravljati in nadzorovati skozi življenjski cikel. Upravljanje identitete mora tudi preprečiti nepooblaščne spremembe v identiteti ter jo tudi nenehno validira oziroma preverja njeno

veljavnost in pravilnost. In, ne nazadnje, upravljanje identitet mora zagotavljati tudi varno uporabo identitete v realnem času, torej jo distribuira varno in dovolj hitro.

Izzivi upravljanja identitet ležijo torej predvsem v vzpostavitvi enostavnega mehanizma za obvladovanje kompleksnih relacij med identitetami ter celostno skrbi za veljavnost in pravilnost identitet. Rešitve morajo torej ponujati predvsem sledeče:

- ustvarjanje jasne in unikatne identitete za vsakega uporabnika,
- poenostaviti in racionalizirati okvir in povezave entitet povezane z identiteto,
- definira politiko in varnostne mehanizme profilov.

Rešitve za upravljanje identitet nudijo orodja za načrtovanje in obvladovanje kompleksnih relacij med entitetami in sistemi. Avtomatizirana opravila v orodju ustvarjajo in obnavljajo relacije, ko se uporabniki dodajajo, odstranjujejo, spreminjajo itd. Uporabnikom omogoča dostope do raznih sistemov skozi validirane postopke distribucije konfiguracij, delegiranja pravic, preslikavanja pristnosti in avtorizacij na povezanih sistemih (na primer dostop do strežnika elektronske pošte do podatkov v podatkovni bazi itd.)

Upravljanje identitet, kot ga bom obravnaval v tem delu, učinkovito upravlja celovito identiteto uporabnika in mu zagotavlja hiter in varen dostop do podatkov in storitev (aplikacij), ki jih potrebuje. Reed predstavi naloge upravljanja identitet kot štiri A-je (Reed, 2002, str. 7):

- avtentikacija (Authentication) – kdo je uporabnik?
- avtorizacija (Authorization) – do česa lahko dostopa uporabnik?
- kontrola dostopa (Access control) – upravljanje sredstev za dostope
- revizija (Audit) – poročanje in revizija dostopov

Večina jih še vedno meni, da naj bi taka rešitev bila centralizirana v eni podatkovni bazi, kar pa ni nujno in je rešitev lahko kljub temu učinkovita. Sicer je tako rešitev, ki je centralizirana, lažje upravljati, a ima zaradi tega tudi omejitve, še posebno, ko želimo upravljanje identitet razširiti izven obsega podjetja ali združbe. Takrat govorimo o **zveznem upravljanju identitet**, ki ga bom podrobneje opisal še v nadaljevanju.

1.1.2 Prednosti upravljanja identitet

V uvodu sem že povedal kar nekaj prednosti, ki bi jih način upravljanja identitet prinesel predvsem v poslovno okolje. Na prvem mestu je seveda znižanje časa, potrebnega za

izvedbo nalog in posledično stroškov s povečanjem obsega avtomatizacije skozi pravila in avtomatske procese. To zmanjšuje količino dela pri pomoči uporabnikom, administrativnih delih in tehnični pomoči. Gre tudi za znižanje stroškov celotnega upravljanja ter hkrati povečanje konkurenčne prednosti z uporabo pospešenih avtomatiziranih procesov. Dosegamo lahko tudi boljše storitve na področju skrbi za stranke (angl. *customer care*), odnose med zaposlenimi, strankami in dobavitelji. Za hitrejšo izvedbo organizacijskih sprememb skozi avtomatizirane procese se določijo vloge, ki jih potem samo povežemo z identiteto in avtomatski proces poskrbi za varno in pravilno dodelitev dostopov do informacij na vseh potrebnih področjih. Torej poskrbi za časovne prihranke kot tudi prihranke zaradi človeških napak in površnosti pri izvedbi.

Poleg časovnih, finančnih in varnostnih prihrankov pa lahko omenimo še posebnost, ki se je v praksi pokazala pogosto kot pereč problem: dostop do informacij osebam, ki jim je dostop pretekel ali bil ukinjen (bodisi menjava delovnega mesta, menjava področja dela itd.) Občasno se razne dostope do sistemov omogoča zaposlenim še nekaj časa po ukinitvi zaradi zaključevanja odprtih nalog – vendar se pogosto dostop ne odstrani, ker nihče ne poskrbi za periodično odstranjevanje dostopov (razen seveda v sofisticiranih službah, kjer se to izvaja dosledno s papirno sledjo). Ta problem je zelo pogojen z naravo informacij, do katerih ima oseba dostop. V podjetju Krka, d. d., je nekaj strogo varovanih informacij, ki ji zagotavljajo konkurenčno prednost ali pa jo ogrožajo, če ima dostop do njih nepooblaščen oseba. Ne nazadnje pa sam način strukturiranega dela in definiranih pravil hkrati prinaša tudi sistematizacijo po mednarodnih standardih in priporočilih, kar prinaša še dodatno konkurenčno prednost podjetja v smislu skladnosti z zakonodajami in raznimi mednarodnimi priporočili in direktivami (na primer European Data Protection Directive).

Rešitve upravljanja identitet, če jih izvedemo pravilno, vključujejo in/ali podpirajo več standardiziranih varnostnih mehanizmov, kot so:

- navidezna zasebna omrežja (VPN),
- infrastruktura javnih ključev (angl. *Public Key Infrastructure* – PKI),
- enotna prijava (angl. *Single Sign-On*, v nadaljevanju SSO),
- uporabo imeniških storitev (angl. *Domain Name Services* – DNS),
- kontroliran dostop do korporativnih podatkov,
- standardiziran način upravljanja dostopov (na primer vmesnik za aplikativni dostop do upravljaljskega modula).

Upravljanje identitet je še toliko bolj dobrodošlo pri razdrobljenih mednarodnih podjetjih, na tem mestu pa lahko izpostavim razne zdravstvene institucije, za katere je običajno, da so razpršene na več lokacijah, imajo več dobaviteljev, več partnerjev itd. Lahko predstavljamo pacienta, ki ima več različnih terapij po različnih lokacijah, prehaja od zdravnika do

zdravnika in sama dokumentacija o pacientovih posegih, terapijah ipd. mora potovati skupaj s pacientom in je tako zelo izpostavljena vplivom na tej poti. Posledice netočne ali manjkajoče dokumentacije o pacientovi zdravstveni preteklosti so lahko seveda usodne. Upravljanje identitet v takem primeru skrbi tudi zato, da je takšna dokumentacija vedno na voljo zdravniku, ki je pooblaščen za zdravljenje tega pacienta in da je dokumentacija točna in popolna.

Še ena prednost upravljanja identitet je tudi elektronska oblika večine, če ne kar vseh dokumentov, ki jih v procesih uporabljamo. Proces prehoda v digitalno upravljanje identitet je pogosto počasen in zahteven proces, ki pa v končni fazi prinaša veliko prednosti pri samem upravljanju, skladnosti s standardi (na primer v ZDA morajo bolnice delovati po točno določenem standardu, ki ga predpisuje HIPAA², ki predvideva kako in na kakšen način pripravljati in voditi zdravstveno dokumentacijo o pacientu). Bolnišnice, ki ne prevzamejo novega načina vodenja dokumentacije, enostavno ne morejo več poslovati – torej je prehod nujen.

Poleg prednosti, ki jih prinaša upravljanje identitet, pa seveda prinaša tudi nekaj **nevšečnosti**. Te se predvsem kažejo v kompleksnem planiranju sistema upravljanja identitet, ki se povezuje s »podrejenimi« sistemi, ki pa vsak zase kreirajo neko novo identiteto uporabnika, ki jo potem povežemo z osnovno identiteto (na primer identiteta osebe, ki ima dostop do elektronske pošte – torej povezan sistem elektronske pošte ustvari identiteto uporabnika, ki predstavlja njegov elektronski poštni naslov). V primerih, kjer imamo v sistemu razdrobljeno delegiranje pravic (na primer pravice na določenih skupnih datotečnih sistemih – razdrobljene delegirane pravice) potem si lahko predstavljamo kako kompleksen postane spisek vseh pravic določenega uporabnika in če le-te upravljamo ročno, se tudi verjetnost napake eksponentno povečuje s povečevanjem kompleksnosti. Verodostojnost takih informacij je seveda vprašljiva in po vsej verjetnosti netočna. Če razširimo kompleksnost izven enega podjetja še na partnerje, dobavitelje itd., vidimo, da je možnosti za nepooblaščen dostop do informacij ali napačno dodeljenih pravic »pravemu« uporabniku bistveno več zaradi povečane kompleksnosti in števila sistemov, ki jih želimo upravljati.

Projektni vodje pri implementaciji novih sistemov pogosto nižajo same stroške projekta tako, da prelagajo povezljivost sistema (predvsem kar se tiče upravljanja uporabnikov) z drugimi sistemi. Razlogi za to ležijo v poenostavljanju trenutnega projekta z miselnostjo, da se integracija lahko izvede kasneje – kar pa v bistvu pomeni, da sam sistem ni pripravljen za kompleksna okolja večjih organizacij (angl. *enterprise-ready*), torej ni pravilno povezljiv z ostalimi sistemi. Novi sistemi so redko avtoritativni vir za uporabniške podatke, zato je smiselno pričakovati, da bodo podatki o uporabnikih črpani iz nekega

2 HIPAA je kratica za Health Insurance Portability and Accountability Act (v ZDA)

drugega sistema. Poraja se vprašanje, kako je s posodobitvami podatkov. Ali se popravki v enem sistemu avtomatsko preslikajo v drug sistem? Kje so shranjeni avtoritativni podatki in kdo ter skozi kateri sistem ima pravico posodabljanja? Kakorkoli že, potreba po povezljivosti sistemov je nujna bodisi skozi sistem upravljanja identitet (celostno) ali povezovanje glede na vsak sistem posebej, kar pa dolgoročno namiguje na ponovno konsolidacijo, ko se podjetje zaradi kompleksnosti odloči vpeljati sistem upravljanja identitet.

1.1.3 Organizacijski in tehnični pristop k upravljanju identitet

Upravljanje identitet mnogi vidijo predvsem kot tehnični izziv, kar pa nikakor ne drži. Sistem upravljanja identitet je računalniški program, ki ima svojo nadzorno ploščo, preko katere potem lahko nastavljamo pravice uporabnikov in ob določenih terminih (po urniku) se nastavitve prenesejo na ostale povezane sisteme. Čeprav je v zelo grobem pogledu to dejansko res, pa sistem upravljanja identitet ni samo tehnični problem.

Dobra strategija upravljanja identitet posega globoko v samo organizacijsko strukturo, zajema projekte in sisteme, opredeljuje procese delegiranja pravic, postopkov itd. Upravljanje identitet ni samo tehnični problem ali tehnična rešitev, saj zajema tako celostno organizacijo in relacije med entitetami. Doprinos sistema upravljanja identitet ni koristen samo za tehnike temveč tudi organizatorje in upravljavce podjetij. Podrobneje bom relacijo med tehniko in organizacijo sistemov upravljanja identitet razložil še v nadaljevanju.

V večini dojemamo sisteme upravljanja identitet kot tehnične projekte in izzive, a so dejanski cilji navadno zelo poslovno usmerjeni in zajemajo naslednja področja:

- skladnost projektov s poslovnimi cilji;
- lastništvo in skrbništvo podatkov;
- celovitost, zaupnost, varnost in razpoložljivost podatkov;
- politične in pravne omejitve (pomisleki);
- skladnost in podpora poslovnim procesom.

Na kratko pa naj omenim še nekaj tipičnih razlogov za neuspeh implementacije takih sistemov:

- pomanjkanje razumevanja – bodisi nerazumevanje ciljev, ki jih želimo doseči ali celo nerazumevanje relacij med poslovnimi in tehničnimi cilji projekta;

- pomanjkanje podpore vodstva;
- pomanjkanje varnostnih mehanizmov, ki bi zagotavljali varno uporabo takih sistemov v realnem času;
- pomanjkanje podrobnega planiranja tako poslovnih kot tehničnih izzivov;
- težave pri povezljivosti geografsko ločenih enot podjetij;
- prehod med »stebrnim« načinom poslovanja in »projektnim« načinom – pogosto so stebri (na primer finančna služba, kadrovska itd.) uporabljali lastne programe za izvedbo del, ki pa niso povezljivi z drugimi programi ipd.

Sistemi upravljanja identitet so mnogo več kot samo tehnični izziv. Potrebno je veliko sodelovanja vseh oddelkov in usklajevanja, preden prvi posamezniki šele začutijo prednosti upravljanja identitet. V Krki je zdaj že dobri dve leti v uporabi postopno implementiran sistem upravljanja identitet, ki se še vedno razvija in raste, a prve prednosti še že čutijo.

1.1.4 Funkcionalnosti sistemov upravljanja identitet

V nalogi se bom večkrat vračal k varnostnim mehanizmom in samemu poteku procesa upravljanja identitet, za zdaj pa je dovolj, da si zapomnimo, da je vpeljan proces upravljanja identitet veljaven in obsega tako zaposlene, stranke, partnerje in ne nazadnje tudi aplikacije (sisteme).

V začetkih drugega tisočletja, ko so nastajali prvi sistemi upravljanja identitet, je veljalo enostavno prepričanje o povezljivosti sistemov zgolj po tehnični plati in le malo energije je bilo usmerjene v organizacijo upravljanja. Kmalu so se dodelali tudi organizacijski aspekti projektov, a vendar omejeno in predvsem znotraj enega podjetja, brez povezljivosti z zunanjimi sistemi ali drugimi podjetji. Obsežnejše rešitve upravljanja identitet zajemajo danes tudi t. i. **zvezno identiteto** ali **federativno identiteto** (angl. *Federated Identity*). Zvezna identiteta je postala nujna z vzponom interneta (Windley, 2005, pogl. 12). Danes živimo v času polnega razmaha interneta, kjer imajo dostop do interneta praktično 24 ur na dan vse novejšie mobilne naprave, ki omogočajo povezljivost iz kateregakoli urbanega področja. Čeprav se dostop do interneta pogosto smatra kot anonimni dostop, pa je vseeno potrebno vzpostaviti identiteto, ko želimo opravljati določene interakcije (na primer nakup, prodaja itd.). Oblika identitete, ki jo želimo vzpostaviti, mora biti torej prenosljiva izven meja podjetja. Koncept zvezne identitete definira to identiteto kot tako, ki je sposobna razširiti profil uporabnika do zunanjih partnerjev, ki lahko dostopajo do informacij v podjetju in po drugi strani tudi omogočajo projiciranje uporabnikove identitete izven podjetja.

O zveznih identitetah bom govoril še v nadaljevanju, čeprav se bom predvsem posvečal upravljanju identitet znotraj večjih podjetij (angl. *Enterprises*). Ključna področja vsakega upravljanja identitet v podjetjih bom predstavil v naslednjih podpoglavjih.

1.1.4.1 Življenjski cikel računov

Pojem življenjskega cikla računa predstavlja nenehno skrb za ustvarjene račune v nekem sistemu, bodisi so to osebni, servisni ali sistemski računi. Za račune se vodi zgodovina sprememb in dostopov, torej mora evidenca obstajati tudi po ukinitvi računa. Ključni elementi življenjskega cikla računov so: dodeljevanje in razpuščanje, samopostrežba in delegirana administracija. Skrb za življenjski cikel računa se vedno izvaja, ne glede na dostopne pravice.

1.1.4.2 Upravljanje profilov

Z upravljanjem profilov želimo doseči upravljanje identitet samih in nato prenos informacij izven obsega podjetja – torej v zunanje podatkovne baze, imenike in aplikacije skozi celotno podjetje in izven njega (po potrebi). V tem procesu je zajeto samoupravljanje uporabniškega profila kot tudi avtomatiziran prenos natančnih podatkov v ostale ključne sisteme podjetja.

Za pridobivanje točnih podatkov o profilih je potrebno definirati prave izvore podatkov ter jih ustrezno preslikati skozi pravila in postopke tako, da se ob vsakem kasnejšem popravljanju podatkov le-te informacije pravilno in hierarhično prenesejo v vse dotične izvirne sisteme. Upravljanje profilov mora torej zajemati tudi varnostne mehanizme, predvsem zaradi preprečevanja podvojenih identitet. Ključni sestavni deli upravljanja profilov so: kreiranje in upravljanje unikatnih uporabniških identitet, samoupravljanje uporabniških profilov in avtomatizirana razpršitev teh informacij v ostale povezane sisteme.

1.1.4.3 Delovni tok

Delovni tokovi so vsakdanjik vsakega dela danes. Delovni tok predstavlja neke ustaljene predpise, torej kako se izvajajo določene naloge po vnaprej predvidenih postopkih. Upravljanje identitet v veliki meri sloni in se izvaja po vnaprej pripravljenih postopkih. Za oris si lahko zamislimo delovni tok nekega poslovnega dokumenta: prvotno nastane osnutek dokumenta, ki ga nekdo pripravi ter ga posreduje naprej v pregled, dokument se po pregledu lahko vrne v popravek ali pa potuje naprej s tokom v potrditev, lektoriranje,

dopolnjevanje in končno v objavo (tak bi bil v grobem in zelo na kratko poenostavljen proces nastanka nekega dokumenta). Vsak korak na vmesni poti ima definirano osebo, ki opravi ta korak in to gre vse do zadnje odobritve pred objavo, ki jo na primer potrdi vodja ekipe. Večina današnjih orodij za vodenje dokumentacije (ali dokumentacijski sistemi) imajo vgrajene »delovne tokove«. V Krki je v uporabi istoimenski izdelek podjetja *Documentum* kot glavni dokumentacijski sistem za najbolj pomembno dokumentacijo, ki ima pravila nastajanja in življenjskega cikla dokumenta definirana zelo strogo. Poleg tega pa tudi intranet orodje *Microsoft SharePoint Portal Server*, ki omogoča »delovne tokove«, vendar jih pri nas ne uporabljamo (ker tudi ne uporabljamo *SharePoint* kot dokumentacijski sistem, si pa želimo *SharePoint* uporabiti kot skupna delovna področja oddelkov, za kar pa si tudi želimo upravljanje skozi sistem upravljanja identitet).

Delovni tokovi ponujajo predvsem možnost odobritev korakov v procesih. Torej vsak korak, ki ga mora odobriti nadrejeni, je predviden kot posebna akcija v postopku in ima tudi predvidenega odobritelja in namestnika. Delovni tokovi so lahko zelo enostavni ali pa se zaplete pri dolgih in kompleksnih postopkih, v večini pa njihovo agilnost opredeljuje tudi količina potrditev na sami poti dokumenta. Iz prakse vemo, da se pogosto čaka predvsem na določene potrditve nadrejenih in je ključno, da se za osebe, ki izvajajo potrjevanje in odobritve, ta segment izvede čim bolj prijazno in za uporabnika enostavno in razumljivo. To pogosto pripomore pri zmanjšanju čakalnih dob. Sami delovni tokovi morajo biti implementirani tako, da se torej zavedajo identitete uporabnika, zavedajo konfliktov, ki nastanejo na poti ter jih tudi uspešno rešujejo, nenazadnje pa naj bi tudi predvidevali ročne popravke v primerih, ko je to potrebno.

1.1.4.4 Dodeljevanje pravic in razpuščanje

Dodeljevanje (angl. *Provisioning*) je zelo zanimivo področje, ki se dotika tako upravljanja identitet kot tudi varnosti na področju upravljanja identitet. Dodeljevanje v računalniškem žargonu pomeni dejansko »dodeljevanje pravic« oziroma omogočanje dostopa uporabnikom do določenih vsebin. Varnost povečujejo s tem, da uporabnikom tudi odvzemajo pravice, ko jih le-ti ne potrebujejo več.

Pogosto se tudi uporablja beseda *eProvisioning*, ki namiguje na to, da se ukvarja predvsem z elektronskimi sistemi in dostopi do njih. Ker računalniški sistemi niti ne morejo upravljati nekaj ne-računalniškega, je torej pojem *eProvisioning* zgolj prepoznaven kot marketinški izraz.

Takšne sisteme je včasih težko ločiti od meta-imenikov (opis v nadaljevanju), saj je obema sistemoma skupno, da omogočata dodeljevanje pravic. Kot bomo še spoznali v nadaljevanju, so meta-imeniki bolj primerni za jedro naprednega dodeljevanja pravic,

medtem ko pa širše dodeljevanje pravic ponuja nekaj več storitev kot pa sami meta-imeniki v osnovi, predvsem delovne tokove, upravljanje poslovnih procesov, delegiranje administracije, samopostrežne vmesnike za upravljanje, poročila itd. Vpeljevanje sistemov za dodeljevanje pravic je navadno zapleteno in zahteva tudi revizijo vseh podatkov in računov ter definiranje procesov.

Prednost avtomatskega dodeljevanja pravic se najbolj izrazito opazi pri novo zaposlenih, saj ne morejo začeti z delom dokler niso urejene pravice in dostopi (na primer prijava v računalnik, elektronska pošta, dostop do skupnih map oddelka itd.). Po klasični metodi pride zahtevke za spremembo do posameznega skrbnika sistema, ki potem opravi potrebne nastavitve v sistemu, ki omogoči dostop do vsebin novo zaposlenemu. Če je sistemov veliko, so si med seboj hierarhično povezani, zato pa se lahko čakalne dobe hitro povečajo (na primer skrbnik aktivnega imenika potrebuje določen čas, da naredi uporabniško ime za novo zaposlenega, šele nato preda podatke skrbniku sistema elektronske pošte, ki nato zopet porabi določen čas, da temu uporabnik kreira poštni nabiralnik in ga doda v potrebno oddelčno skupino).

Dodeljevanje pravic torej v veliki meri opredeljuje avtomatsko nastavljanje pravic v podrejenih sistemih po vnaprej pripravljenih postopkih. Običajno se ta proces za novo zaposlenega začne v kadrovske službi, kjer vnesejo njegove podatke v sistem ter mu določijo delovno mesto in vloge. Sistem za dodeljevanje pravic nato kreira potrebne uporabnikove identitete v vseh povezanih sistemih. Stroški, ki so povezani z dodeljevanjem pravic na tak način, močno upadejo, po drugi strani pa se bistveno poveča hitrost izvedbe in tudi pravilnost (varnost) izvedbe. Uporabniki sistematično pridobijo vse potrebne dostope in pravice z zelo zmanjšano stopnjo možnosti napake.

1.1.4.5 Delegirano upravljanje

Delegirano upravljanje je pomembno predvsem za velika okolja, ki so povezana z dobavitelji, strankami in tudi zaposlenimi. Samo delegiranje se začne pri določitvi računov (uporabnikov), ki lahko opravljajo določena dela, za katera so predvideni ali imajo pooblastila.

Samo delegiranje pravic je tehnično precej zahteven proces, saj je potrebno dobro razdelati modele pravic in dostopov ter tudi nadzor nad delovanjem teh modelov. Uporabniki smo bili do zdaj (vsaj pred prihodom operacijskih sistemov Windows Vista oziroma Windows 7) navajeni delati na računalniku v okviru skrbnika (Administrator), kar nam je omogočalo nameščanje naprav, spreminjanje sistemskih nastavitev itd. brez vnaprejšnjega obvestila »da delamo v kontekstu skrbnika«. Danes je filozofija obrnjena, saj vsak uporabnik dela na računalniku kot »uporabnik« in šele, ko hoče izvesti akcijo kot »skrbnik« sistema, ga le-ta

obvesti, če želi izvesti to akcijo, saj mora preiti iz konteksta navadnega uporabnika v skrbniški kontekst (začasno). Temu lahko na kratko rečemo tudi začasno delegiranje pravic – podobno velja tudi v sistemih upravljanja identitet, kjer poznamo začasno delegiranje pravic (kot v primeru) ter trajno, kar pa bolj sovпада s pojmom vloge (torej vloga določenega uporabnika je v kreiranju novih uporabniških računov). Primer razdrobljenosti v operacijskih sistemih nakazuje na to, da mora sistem upravljanja identitet poznati razdrobljenosti podrejenih sistemov in v mnogo primerih tudi predvidevati razdrobljenost pravic v »neznanih« sistemih (torej biti dovolj odprt in sposoben prilagajanju neznanim izdelkom).

1.1.4.6 Samopostrežba

Posebna oblika delegiranega upravljanja je »samopostrežna« storitev ali samopostrežba (angl. *self-service*). Prednost samopostrežnih storitev je v tem, da lahko uporabniki v določeni meri sami spreminjajo podatke svoje identitete. To v veliki meri razbremeni predvsem službo za pomoč uporabnikom in posledično lahko prihrani veliko časa in denarja. Samopostrežba je velikokrat implementirana v obliki zahtevkov po dostopih do vsebin. Na primer strežnik Microsoft SharePoint ponuja uporabniku, ki nima dostopa do določene vsebine, da namesto vsebine prikaže obrazec za zahtevo po dostopu do te vsebine. Izpolnjen obrazec se pošlje direktno osebi, ki je odgovorna za konkretno vsebino, ki lahko odobri (in realizira) ali zavrne dostop. Podrobneje razdeljene samopostrežne funkcije omogočajo menjavo gesel, povrnitev pozabljenega gesla ipd.

1.1.4.7 Upravljanje gesel

Gesla pri uporabnikih so pogosto velik problem, tako varnostni (prekratka gesla niso varna, predolga in kompleksna pa zopet ne, ker si jih uporabniki raje zapišejo v bližino računalnika, kot pa tvegajo, da geslo pozabijo – kar je spet varnostno sporno. Prava težava pa nastopi, ko imajo uporabniki različna gesla (in lahko tudi uporabniška imena) za različne sisteme. To problematiko lahko rešujemo z upravljanjem gesel. Predvsem v Microsoft okoljih (kot je tudi Krka) je upravljanje gesel že deloma urejeno skozi aktivni imenik, in če je ta na najvišji ravni oziroma avtoritativen za naše okolje, potem je potrebno samo orodje za menjavo gesel predstaviti kot centralno orodje za menjavo gesel, v nasprotnem primeru pa je potrebno izvesti hierarhijo sistemov in pripraviti vmesnik za menjavo gesel, ki potem skozi definiran proces tudi menja geslo na podrejenih sistemih. Sama gesla so v takih primerih lahko shranjena bodisi v centralni bazi podatkov ali pa razpršena po individualnih sistemih – odvisno od tehnične rešitve. V primeru razpršenosti potrebujemo sinhronizacijsko storitev (del dodeljevanja). Obe metodi imata enak rezultat, čeprav druga zahteva nekoliko več dela v smislu priprave algoritmov in sinhronizacijskega

servisa. Prednost upravljanja gesel je nedvoumno hitrost, varnost in znižanje stroškov poslovanja. Pogosto pa srečamo kombiniran način, saj na primer aktivni imenik že sam neposredno omogoča uporabo enotnega gesla in uporabniškega imena v mnogih sistemih, ostale pa se lahko nato poveže s sinhronizacijsko storitvijo.

1.1.4.8 Nadzor dostopa na podlagi vloge

Nadzor dostopa na podlagi vloge (angl. *Role Based Access Control*, v nadaljevanju RBAC) je sistem, ki je danes zelo razširjen in tudi zelo dobro podprt s standardi. Sistem je namenjen avtomatizaciji dodeljevanja dostopov identitetam do storitev (sistemov) v podjetju na podlagi vnaprej pripravljenih vlog na sistemu. RBAC standardi so razviti za več področij: vojaško, zdravstveno, industrijsko, biometrično in splošno področje. Na trgu prisotni ponudniki IdM sistemov ponujajo RBAC za splošna področja, kar je predvsem namenjeno večjim podjetjem, kjer so vloge zaradi kompleksnosti sistemov nujno definirane vnaprej.

Do leta 2004 so bili RBAC standardi definirani pomanjkljivo in slabo, nato pa je ANSI predstavil nov standard na tem področju, modeliran po NIST³ modelu (ANSI INCITS 359-2004, str. 2-9), ki je danes osnovni standard za splošne namene. Sam NIST model pa je bil opredeljen že leta 2000 in se nenehno izpopolnjuje (Ferraiolo & Kuhn & Sandhu, 2000). Sam RBAC standard je definiran zelo brezoblično (amorfno), kar pomeni, da je zelo dojemljiv za prilagoditve in kot tak zadostuje za večino primerov. Čeprav je bilo razvitih in predstavljenih več različnih modelov poleg RBAC modela, pa le-ti niso relevantni za predstavitev v tej nalogi, zato bom samo opisal RBAC model (Ferraiolo & Kuhn, 2004, str. 3).

Osnovni koncept RBAC je vzpostaviti dostope in pravice do sistemov na podlagi vlog. Naslednji korak je dodelitev vlog uporabnikom v sistemih. Same vloge v podjetju so lahko definirane na podlagi delovnih mest, organizacijske strukture, nalog, odgovornosti in drugega (Ferraiolo et al., 2000, str. 1).

NIST model je osnova za standardni referenčni model RBAC, ki temelji na uporabi dveh tipov pravic (negativne in pozitivne), kjer pozitivne pomenijo odobren dostop, negativne pa zavrnjen dostop. Tak model je neodvisen od same narave vlog ter tudi ne opredeljuje načinov avtentikacije in avtorizacije. Poznamo štiri nivoje RBAC:

Linearni RBAC. Predstavlja osnovni pogled na nadzor dostopa na podlagi vloge in predvideva, da ima vsaka entiteta lahko poljubno število (1..*) vlog, prav tako pa ima

3 NIST je kratica za National Institute of Standards and Technology

lahko ena vloga tudi več pravic (na več ali enem sistemu). Torej tak način tudi ne izključuje uporabniku možnosti dodeljevanja tudi drugih vlog iz drugih sistemov (Ferraiolo & Kuhn, 2004, str. 11).

Hierarhični RBAC. Zelo je podoben linearnemu, loči pa ga uvedba hierarhije za vloge. Sama hierarhija vlog je v bistvu naravni način strukturiranja vlog, saj so si v podjetjih večinoma vloge v enakem področju podrejene in nadrejene ena drugi. Pri sami zasnovi hierarhičnega modela pa sta nastali dve izvedbi: neomejen ali **splošni hierarhični model** (podpira neomejeno število vlog, ki opisujejo hierarhijo) in **omejen hierarhični model**, ki pa vsebuje omejitve v strukturi hierarhije vlog. V večini primerov so hierarhije omejene na preprosta drevesa (Ferraiolo & Kuhn, 2004, str. 17).

Omejen RBAC. Ker si modeli sledijo kot logične nadgradnje prej omenjenega modela, izvira omejen RBAC iz hierarhičnega in mu dodaja omejitve. Omejitve so lahko statične in se navezujejo na relacije med uporabniki in vlogami ali dinamične, ki se navezujejo na aktivacijo vlog znotraj uporabnikove seje. V bistvu omejen model predvideva izločevanje vlog med seboj. Na primer če ima uporabnik določeno vlogo na sistemu, potem ne more imeti določene druge vloge, ker mu pravila preprečujejo dodelitev dveh izključujočih se vlog. Za omejen RBAC model se pogosto uporablja tudi izraz **SoD** (angl. *Separation of Duties*) ali ločevanje nalog (Ferraiolo & Kuhn, 2004, str. 21).

Simetrični RBAC. Zadnji model pa poskuša reševati problem nadzora nad relacijami med vlogami in pravicami. Simetrični RBAC nadgrajuje omejen RBAC s pogledom, ki služi kot orodje za pregledovanje pravic dodeljenih vlog ali uporabnikom. Na ta način si lahko v podjetju izdelajo poglede, ki jim izpostavljajo pretekle vloge uporabnikov, nepotrebne vloge uporabnika, ko menja delovno mesto ipd. Poleg tega pa simetrični RBAC omogoča še nekaj dodatnih pogledov na pravice, kot so neposredno ali posredno (preko hierarhije vlog) dodeljene pravice in poglede preko različnih sistemov (Ferraiolo et al., 2000, str. 10).

1.1.4.9 Revizija in poročanje

Že v začetku poglavja sem omenil štiri A-je (avtentikacija, avtorizacija, kontrola dostopa – *access*, revizija – *audit*). Prve tri postavke sto tradicionalni varnostni mehanizmi, ki se uporabljajo pri prijavi uporabnikov v sistem (preverjanje pristnosti, avtorizacija in dostopne pravice), medtem ko ima revizija lahko celo širši pomen. Vsi štirje A-ji so pomembni pri upravljanju identitet.

Preverjanje pristnosti pomeni sistem prijave, torej pravilno identifikacijo uporabnika (na primer njegovo uporabniško ime, prstni odtis itd.), avtorizacija predstavlja proces, ki potrdi

ob pravilni prisotnosti tudi vsebinski dostop do informacij. Avtorizacija v grobem preverja, ali je uporabniški račun omogočen in veljaven, medtem ko pa dostopne pravice povejo, do katerih informacij ima ta uporabnik dejansko dostop.

Podjetja, podvržena raznim mednarodnim standardom, morajo že dalj časa pripravljati take ali drugačne oblike poročanja in revizije dostopov. Posledično se prej opisane akcije vedno tudi beležijo v sistemske dnevnike. V kolikor dostop do teh dnevnikov ni urejen ali ne omogoča izdelave poročil, kaj in kdaj je bilo narejeno in tudi oblike poročil v smislu kdo ima dostop do kje, to ne predstavlja sistema poročil in revizij. Šele, ko zagotovimo učinkovit sistem poročil, ki omogoča tudi revizijo in revizijsko sled, lahko govorimo o vpeljavi vseh štirih A-jev (Reed, 2002, str. 7):

1.1.5 Standardi na področju upravljanja identitet

Ne glede na to, da so standardi o upravljanju identitet prisotni že od 80. let dalje, je to področje v praktičnem smislu še vedno relativno mlado, saj se veliko podjetij šele danes prvič spopada s težavo upravljanja identitet, ali pa so (kot podjetje Krka, d. d.) vpeljali šele prvo fazo projekta upravljanja identitet, ki predvsem zajema pripravo infrastrukture in nekaj osnovnih sistemov (uporabniški računi, skupine, elektronsko pošto itd.).

Standardi so prisotni že od začetka vzpostavitve omrežij, saj je bilo potrebno definirati, kako bodo posamezna vozlišča omrežja komunicirala med seboj. Standard X.500 ponuja mehanizem za predstavljanje identitet širom po svetu že od leta 1984 in je redno posodobljen in izpopolnjen ter se še vedno uporablja, vendar predvsem v vladnih in izobraževalnih ustanovah. Bolj razširjen znotraj podjetij je LDAP, ki je bil razvit leta 1990, vendar žal ni rešil vseh problemov upravljanja identitet in je samo deloma uspešen in razširjen.

Zaradi pomanjkljivosti teh dveh standardov se je pojavilo kar nekaj iniciativ, ki poskušajo celostno zajeti upravljanje identitet. Pod okriljem organizacije OASIS⁴ so nastali naslednji standardi, ki so danes v uporabi (Reed, 2002, str. 21):

- SAML – *Security Assertion Markup Language* ponuja način varne rešitve avtentikacije in avtorizacije med različnimi sistemi z uporabo XML jezika.
- SPML – *Service Provisioning Markup Language* ponuja način rešitve dodeljevanja uporabniških računov v različne sisteme (angl. *Provisioning*).
- XACML – *eXtensible Access Control Markup Language* ponuja rešitve prenašanja politik dostopov do informacij (na internetu), torej definira kdo, kdaj, kje in kako lahko dostopa do določenih informacij. Kontrola dostopa se pogosto reče tudi »upravljanje

4 OASIS je kratica za angl. *Organization for the Advancement of Structured Information Standards*

pravic« (angl. *Rights management*), kar bistvu pove kdo lahko dostopa do informacij, kaj lahko z informacijo naredi in s katero napravo lahko pride do informacije.

- WS-Security – *Web Services Security*, ki je nastal pod okriljem treh podjetij (IBM, Microsoft in VeriSign), je leta 2002 prešel tudi pod OASIS. WS-Security definira nabor SOAP⁵ razširitev, ki v spletne storitve dodajajo možnost definiranja celovitosti in zaupnosti. WS-security ponuja temelje za varne spletne storitve, ki omogočajo osnovo za nadaljnje višje ležeče storitve, kot so *federacija* in *zaupanje* med različnimi storitvami.

Poleg teh pa naj omenim še uporabne tehnologije, ki predstavljajo globalno upravljanje identitet v internetu, kot so *Microsoft Live*, *Google Account*, *OpenID* in še nekatere druge. Bistvena prednost uporabe ene izmed teh storitev je v tem, da ponujajo »enovite prijave« (angl. *Single Sign-On*) – kar za uporabnike predstavlja predvsem uporabno prednost, saj lahko z eno samo prijavo dostopajo do več storitev. Žal je v večini primerov še vedno prijava vezana na ponudnikove storitve – na primer do *Google Docs* lahko dostopamo samo z Google računom, ne pa tudi na primer z Microsoft Live računom. Prednost ima OpenID, ki je neodvisen od proizvajalca, vendar posledično tudi manj razširjen, saj konkurenca pridobi uporabnike s storitvijo, medtem ko OpenID uporabljajo predvsem tisti uporabniki, ki so se sami že soočili s problemom preveč identitet, ki jih uporabljajo.

Poleg standardov pa je sprejetih tudi nekaj direktiv in zakonov, ki skrbijo za zaščito podatkov in preprečujejo zbiranje določenih podatkov organizacijam. Že od leta 1999 je v veljavi t. i. *Children's Online Privacy Protection Act*, ki preprečuje določenim spletnih stranem zbiranje podatkov o otrocih, mlajših od 13 let, če nimajo dovoljenja staršev. Podobno imamo v Evropi *European Data Protection Directive*, ki izhaja iz angleške direktive s skoraj identičnim imenom in govori o tem, da je vsak dostop do podatkov potrebno zaščititi tako, da je mogoče samo pravim osebam ob pravem času dostopati do podatkov. Ravno zaradi tega pa je potrebno implementirati določene varnostne mehanizme, ki to zagotavljajo. Bistveno sporočilo direktiv in zakonov je, da vsaka država ali podjetje vsebuje določen nabor pravil in politik o tem, kako se do podatkov dostopa, kako se jih hrani ipd. Pri objavi kakršnihkoli podatkov je torej pomembno spoštovanje zakonov v državi, kjer jih objavljamo, zakonov držav, iz kjer dostopajo do podatkov in ne nazadnje tudi internih politik in predpisov podjetij, ki sodelujejo pri izmenjavi (dostopu, objavi) podatkov.

1.2 Upravljanje identitet v Sloveniji

Slovenija v pogledu upravljanja identitet v svetu ne zaostaja prav veliko ali celo ne. Še

5 SOAP je kratica za angl. *Standard Object Access Protocol*

največja omejitev pri vpeljevanju identitet je pogosto velikost podjetja, saj v manjših podjetjih vpeljava takega sistema predstavlja višje stroške, kot pa je kasneje vrnjene investicije. Zakaj tako?

Povedal sem že v uvodu, da je upravljanje identitet zanimivo posebno, ko razmišljamo predvsem o upravljanju zveznih identitet – torej razpršenih več različnih identitet v različnih sistemih. Manjša podjetja imajo praviloma manj sistemov, ki so lažje obvladljivi in imajo pogosto tudi enakega skrbnika. V takem primeru torej upravljanje identitet predstavlja v bistvu res lažjo administracijo, ko je IdM sistem vpeljan, vendar za samo vpeljavo zahteva zelo veliko virov, planiranja in sistematizacije postopkov ter tudi dobro mero infrastrukturnih sprememb, ki jih moramo vpeljati, v kolikor želimo vpeljati sistem za upravljanje identitet. Kot bom predstavil v 3. poglavju naloge, mora podjetje prilagoditi določene infrastrukturne sisteme (kot je na primer Aktivni imenik), da se le-ti lažje in bolj celovito vklopijo v IdM sistem.

Glede na statistični urad Slovenije je bilo v letu 2005 še vedno večina podjetij v Sloveniji »majhnih« in to kar 99 % (tabela 1). V obdobju med leti 1995 do 2005 so v opazovanih dejavnostih (področja C – rudarstvo, D – predelovalne dejavnosti, E – oskrba z elektriko, plinom in vodo, F – gradbeništvo, G – trgovina, popravila motornih vozil in izdelkov široke porabe, H – gostinstvo, I – promet, skladiščenje in zveze ter K – poslovanje z nepremičninami, najem in poslovne storitve) močno prevladovala majhna in srednje velika podjetja (tj. taka, ki imajo do 249 oseb, ki delajo). V letu 2005 je bilo med 88.618 podjetji v opazovanih dejavnostih 278 velikih podjetij, ki so opredeljena kot poslovni subjekti z 250 ali več zaposlenimi.

Tabela 1: Število podjetij v Sloveniji, po velikosti, 2000-2005

LETO	Skupaj	Velikost podjetij glede na število oseb, ki delajo	
		1-249	250+
2000	85.923	85.617	306
2001	85.926	85.625	301
2002	87.316	87.008	308
2003	86.984	86.688	296
2004	89.093	88.813	280
2005	88.618	88.340	278

Vir: Statistični urad republike Slovenije

Torej velikih podjetij, ki imajo več kot 1.000 zaposlenih, je torej še bistveno manj. Ker je to specifična majhna država Slovenije, pa še ne pomeni, da upravljanja identitet manjša podjetja tudi ne poznajo. Eno izmed prvih podjetij, ki je zaznalo tržno nišo in hkrati

usmerilo del svojega produkta v manjša podjetja, je *IBM Tivoli Federated Manager Business Gateway*, ki je v bistvu enostavnejša izvedba njihovega primarnega IdM produkta *IBM Federated Identity Manager*. Produkt prinaša na ravni industrije enotno identiteto za manjše organizacije, ki se preko interneta varno povezujejo z večjimi, in sicer zaradi različnih razlogov, kot sta nakup in prodaja novih storitev, izdelkov, surovin itd. Produkt je prisoten na slovenskem trgu že od leta 2006, vendar podjetja, ki potrebujejo takšen način dela, v naši regiji še vedno niso izrazita. Ker izstopa po namenu predvsem za manjša podjetja, sem ga omenil na tem mestu, čeprav se bom pregledu rešitev posvetil bolj podrobno v drugem poglavju. Tam pa bom predstavil le vodilne rešitve na tem področju.

Zaradi zasebnosti podjetij je zelo težko pridobiti informacije o vpeljanih rešitvah v posameznih podjetjih v Sloveniji, zato sem se odločil za pregled ponudb slovenskih informacijskih podjetij na trgu in njihovih referenc, ter za pregled tipičnih sistemov v izbranih večjih slovenskih podjetjih. Na podlagi teh podatkov bom torej oblikoval seznam najbolj tipičnih sistemov, ki jih želimo upravljati s sistemom upravljanja identitet, ter ocenil stanje v slovenskih podjetjih danes. Na slovenskem trgu se praktično vsako večje IT podjetje danes tudi ukvarja z vpeljavo sistemov upravljanja identitet. V okviru slovenskih univerz je bilo narejenih tudi veliko diplomskih nalog, predvsem v okviru Fakultet za računalništvo in informatiko, kjer so diplomanti predstavili kar nekaj tehničnih rešitev upravljanja identitet v slovenskih podjetjih, kar sovpada tudi z mojimi spoznanji o naboru sistemov tipičnih slovenskih podjetij.

Vsako podjetje je torej sestavljeno vsaj iz kadrovske baze podatkov, ki je danes pogosto zastavljena kot **kadrovski informacijski sistem (KIS)**. Kadrovska baza je že sama po sebi izvedena kot informacijski sistem, torej ima digitalno relacijsko podatkovno bazo kot hrambo podatkov ter uporabniški vmesnik, preko katerega uporabniki vzdržujejo podatkovno bazo. Ima tudi razdelan sistem pravic uporabe podatkovne baze ter nenazadnje tudi sistem upravljanja uporabnikov in pravic. Ta sistem je danes enoten vsem podjetjem tako, da ga zagotovo lahko uvrstimo na prvo mesto. Kadrovski informacijski sistemi so pogosto tehnično izvedeni s strani lokalnega proizvajalca – torej domače izvedbe. Nekatera večja podjetja so kadrovske sisteme tudi že preselila v celovite programske rešitve (angl. *Enterprise Resource Planning*, v nadaljevanju ERP), še bolj pogosto pa so jih s temi sistemi samo povezali.

Poslovni informacijski sistemi so prav tako prisotni pri vseh večjih podjetjih, saj so praktično temeljno orodje obvladovanja poslovanja podjetja. Sama stopnja razvitosti teh sistemov v posameznih podjetjih pa je odvisna v veliki meri od zakonodajnih potreb in tudi od stopnje podvrženosti podjetij določenim standardom. Tu predvsem izstopajo farmacevtska podjetja, ki so podvržena veliko standardom v samem procesu proizvodnje in tudi v načinu poslovanja. Celovite programske rešitve (ERP sistemi) na slovenskem tržišču so tako domače kot tuje proizvodnje. Prednost domačih proizvodov je v prilagojenosti

posameznim zakonskim posebnostim Slovenije. Ta so pogosto bolj prisotna predvsem v javnih podjetjih in deloma v manjših podjetjih, medtem ko večina večjih podjetij z mednarodnim poslovanjem uporablja mednarodne sisteme, ki so tudi bolj prilagojeni takemu načinu poslovanja.

V proizvodnih podjetjih je poleg kadrovske baze prisoten še vsaj podsistem vlog in nalog posameznikov v proizvodnem procesu, torej podpora proizvodnim sistemom. Razvitost **proizvodnega informacijskega sistema** je odvisna od stopnje avtomatizacije procesov v proizvodnji. Vodilna proizvodna slovenska podjetja imajo stopnjo avtomatizacije relativno visoko ter posledično uporabljajo ločene proizvodne informacijske sisteme večinoma tujih proizvajalcev.

Poleg teh osnovnih sistemov, ki so ključni za poslovanje podjetij, pa se v današnjem času pojavljajo še sistemi, ki so tudi ključni z vidika poslovanja, saj omogočajo komunikacijo in sodelovanje zaposlenih. Na tem mestu bi izpostavil sistem **elektronske pošte in telefonije** (čeprav upravljanje sistema telefonije znotraj podjetij, še posebno v času interneta, močno upada, imajo večja podjetja še vedno interno telefonsko mrežo, ki jo upravljajo lastno). Predvsem sistem elektronske pošte v mnogih podjetjih označujejo kot angl. *business critical* sistem oziroma sistem, brez katerega je samo poslovanje podjetja ohromljeno. Pogosto poteka večina komunikacije preko elektronske pošte, poleg tega pa se čedalje bolj pogosto pojavlja uporaba elektronskega poštnega naslova kot **unikatnega identifikatorja** osebe (identiteta), kar pa sistemu daje še poseben pomen.

Sistem elektronske pošte je lahko izveden popolnoma ločeno od uporabniških imen in gesel, ki jih zaposleni uporabljajo, ali pa je izveden povezano – ne glede na izvedbo se samo kreiranje elektronskih poštnih naslovov kreira ločeno od kreiranja uporabniških imen in gesel za uporabo namiznih računalnikov v podjetjih. Zakaj tako? Kljub temu, da ima vsak zaposleni možnost uporabe elektronske pošte, pa vsa uporabniška imena ne predstavljajo dejanskih zaposlenih, saj so lahko računi za avtomatske obdelave podatkov, izvajanje storitev v ozadju ipd. Jasno je, da je **sistem uporabniških računov** in gesel ločen sistem, sistem elektronske pošte pa je lahko kvečjemu podsistem ali ločen sistem. Sistemi, ki hranijo uporabniška imena in gesla (in tudi druge podatke) so t. i. imeniki oziroma najbolj tipična izvedba v Sloveniji je aktivni imenik, ki je storitev Microsoft Windows okolja za podjetja. V poslovnih okoljih v Sloveniji je to tipična izvedba imeniških storitev.

V podjetjih, kjer so prisotni vsi ti sistemi, so pogosto prisotni tudi manjši sistemi, ki izvirajo posledično iz okolja – to so sistemi datotečnih storitev, intranet in ekstranet sistemi, sistemi za urejanje vsebin (angl. *Content Management System* – CMS) itd. V praktičnem delu naloge se bomo posvetili predvsem vpeljavi sistema upravljanja vsebin za sisteme, identificirane kot osnovne in skupne večjim podjetjem.

2. OKOLJE IN SISTEMI UPRAVLJANJA IDENTITET

V prejšnjem poglavju sem predstavil, kaj je upravljanje identitet, kaj zajema in kaj so (v teoriji) ključne funkcionalnosti in storitve, ki naj bi jih sistem upravljanja identitet doprinesel. Spoznali smo, da je problem mnogih identitet prisoten ne samo v digitalnem svetu, temveč ima vsak posameznik danes več identitet, ki predstavljajo točno samo njega (na primer plačilna kartica, vozniško dovoljenje itd.). Ker bi podrobna analiza možnosti uvedbe upravljanja identitet v svetovnem merilu presegla obseg in namen te naloge, se bom odslej predvsem nanašal na velika poslovna okolja in sodelovanje med dvema ali več podjetji znotraj meja Evropske unije. Prav tako se je zelo smiselno osredotočiti na storitve, ki so dovolj zrele za vključitev v upravljanje identitet in dostopov na ravni podjetja ter (še posebno v začetni fazi) izpustiti področja, ki bodisi niso sistemsko urejena ali so tehnično implementirana slabo in bi proces vključitve v IdM zahteval velik programerski napor in tako bistveno zavlekel sam projekt. Projekti uvedbe sistema upravljanja identitet so občutljive narave, saj se neposredno ukvarjajo z dodeljevanjem pravic uporabnikom iz nadzornega sistema na podsisteme. Ključna je torej pravilnost implementacije pravil dodeljevanja, saj imajo napake lahko zelo resne posledice.

V tem poglavju se bom osredotočil na ključne storitve vsakega upravljanja identitet ter okolja, ki so primerna za razmišljanje o vpeljavi sistema upravljanja identitet. Kakšna so minimalna okolja? Kakšne sisteme imajo? Kaj povezovati? To so ključna vprašanja, na katera bom odgovoril v podpoglavjih.

2.1 Okolje, sistemi in potreba po upravljanju identitet

Okolja, ki danes že zahtevajo upravljanje identitet, so prišla do tega spoznanja skozi svojo kompleksnost. Sama ideja enotne identitete je že zelo stara. Izvira tako iz običajnega življenja kot tudi iz poslovnih potreb, kot smo spoznali v uvodu. Teoretično bi se lahko šli upravljanje identitet na svetovnem oziroma meddržavnem nivoju, vendar lahko hitro ugotovimo, da bi, zaradi različnih zakonov in predvsem zaradi »zasebnosti« določenih informacij, bilo tako dejanje praktično neizvedljivo. Postane pa zelo izvedljivo znotraj podjetij, ki svoja pravila prilagajajo potrebam upravljanja identitet ter v določeni meri tudi predvidevajo sodelovanje z drugimi podjetji. Če je sodelovanje mednarodno, potem se lahko pri izmenjavi podatkov zaplete, še posebno, če se določeni zakoni v različnih državah preveč vsebinsko razhajajo, da bi bilo mogoče varno izmenjevati osebne podatke in zadostiti zakonom obeh držav. Pogosto pa se za upravljanje identitet odločajo predvsem velika (in tudi mednarodna) podjetja, ko jim samo upravljanje mnogih različnih računov (entitet) v različnih sistemih predstavlja čedalje večje časovne in varnostne izzive.

Podjetje Krka, d. d., iz Novega mesta je veliko podjetje (tudi mednarodno), ki se je soočilo s težavo upravljanja identitet, predvsem iz časovnega aspekta (dodeljevanje pravic v mnoge podsisteme, dodeljevanje elektronskega poštnega naslova itd.), ki je preseglo neko normalno časovno dobo, v kateri se zahtevki realizirajo. Prvotne želje (kar bom še podrobneje predstavil v nadaljevanju v poglavju Uporabniške zahteve) so bile predvsem pospešitev dodelitve naslova elektronske pošte novo zaposlenim, dodelitev osebne mape novo zaposlenim in dodelitev pravic dostopa do informacij oddelka novo zaposlenega. Pogosto se zgodba o vpeljavi sistema upravljanja identitet začne na zelo podoben način: torej okolje preseže določeno velikost in z razdrobljenim upravljanjem identitet, časovno ne zmore več dohajati zahtevkov po spremembah in jih izvajati v želenem času.

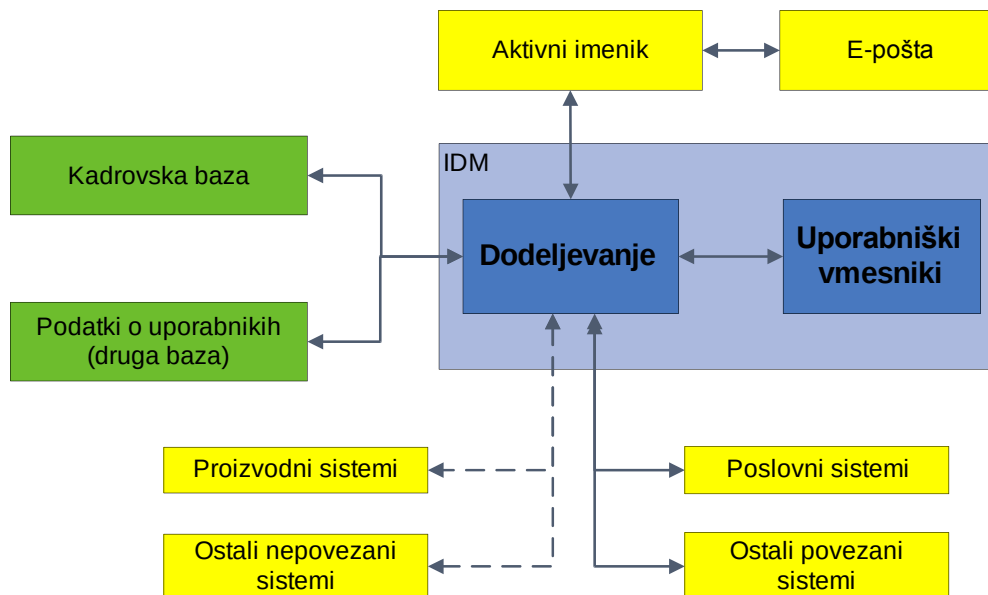
2.1.1 Okolje

Okolja, v katerih bomo obravnavali sisteme za upravljanje identitet, so torej velika poslovna okolja, ki nas predvsem zanimajo ob vpeljavi sistemov upravljanja identitet v poslovno okolje velikega mednarodnega podjetja. Čeprav lahko o upravljanju identitet govorimo že v bistveno manjših okoljih, pa morda le-ta niso toliko zanimiva s stališča manjšega števila zaposlenih kot tudi s stališča manjšega števila storitev in sistemov, ki jih uporabljajo – posledično torej za nas manj zanimiva, saj želimo definirati sisteme upravljanja identitet za čim širše področje delovanja – torej tako, da pokrije čim več, če ne kar vse, storitve v podjetju (čeprav praktično noben IdM sistem ne pokrije *vseh* sistemov v podjetju).

Okolje je tako predvsem oblikovano s količino objektov, ki ga sestavlja (osebe, objekti, lokacije itd.), z njihovimi relacijami (odnos med objekti) in vlogami (kaj so naloge posameznih zaposlenih ter hierarhično strukturo), tipično umestitev prikazuje slika 2. Samih objektov v podjetju je bistveno več kot zaposlenih. Če si predstavljamo, da vsak zaposleni predstavlja en objekt v kadrovske bazi, ima ta objekt še svoj nabor relacij – na primer je podrejen določeni osebi (vodji), je član določene skupine (oddelčne skupine), ima definirano določeno delovno mesto (lokacija), dostope do drugih lokacij itd. V manjših podjetjih obstajajo enaki objekti in relacije, razlika pa je predvsem v kompleksnosti. En skrbnik lahko upravlja kar nekaj različnih sistemov in ob primerni količini podatkov sami IdM sistemi niti niso potrebni – predvsem je to opazno pri manjših podjetjih, ki nimajo težav pri obvladovanju manjšega števila zaposlenih in relacij med njimi. Navadno uporabljajo tudi manjši nabor sistemov in storitev v podjetju, kjer jim na primer zadovoljivo upravljanje nudi že sam vmesnik za aktivni imenik (kot primer lahko vzamemo podjetje, ki uporablja Windows domeno z aktivnim imenikom – posledično lahko skrbnik določa dostope do določenih vsebin – na primer, do datotečnih storitev), vendar ne omogoča enotnega načina dela – torej za vsak podsistem obstaja navadno lastno orodje, aktivni imenik pa omogoča upravljanje določenih (v tem primeru) Microsoftovih

tehnologij, prav tako se ne da definirati avtomatskih procesov delegiranja pravic ipd.

Slika 2: Tipična umestitev sistemov IdM in povezava na druge sisteme



Vir: Interna dokumentacija Krka

Samo okolje pa je tudi zelo pogojeno z naravo podjetja, saj na primer pri avtomatizirani proizvodnji podjetja razmišljajo o upravljanju identitet tudi v proizvodnem okolju, medtem ko storitvena podjetja tega segmenta ne uporabljajo niti ne potrebujejo. Krka je mednarodno podjetje, ki uporablja velik nabor internih sistemov in storitev. Vpeljava v veliko zrelo okolje se zdi smiselna na prvi pogled, vendar brez podrobne identifikacije sistemov in procesov, ki jih želimo zajeti v upravljanju identitet, ne moremo začeti razmišljati o vpeljavi.

2.1.2 Sistemi in storitve

Ključne sisteme, ki nas zanimajo pri upravljanju identitet v modernih združbah, lahko izluščimo iz nabora vseh sistemov v podjetju. Podjetja se ločijo tako po zvrsteh (proizvodno, storitveno, trgovsko ...) kot tudi po obsegu in pestrosti storitev, ki jih ponujajo. V nalogi se bom sicer osredotočil na sisteme, ki jih bomo vključili v sistem upravljanja identitet v podjetju Krka, vendar je najprej potrebno identificirati večji nabor sistemov, ki so skupni več podjetjem, ter nato izbrati avtoritativne vire podatkov in podrejene sisteme.

V poglavju 1.2 smo identificirali sisteme, ki so skupni večjim podjetjem v Sloveniji,

katerih predstavnik je tudi Krka, čeprav v raziskavo ni bila vključena (ni bila izbrana v naključni vzorec). V nadaljevanju pa bom vsak sistem, ki je pomemben za nalogo, predstavil s stališča pomembnosti v Krki.

Kadrovski informacijski sistem (KIS). Vsako podjetje, ne glede na zvrst posla, ima v osnovi zaposlene **osebe** oziroma ljudi, ki predstavljajo kadrovske baze podatkov. Najpomembnejša komponenta kadrovskega sistema je baza podatkov, ki hrani podatke o objektih, ter njihovo hierarhično strukturo (kdo je komu nadrejen/podrejen). V okvir podatkov spadajo ime, priimek, naslov, datum rojstva, EMŠO, datum sprejema, izobrazba, stroškovno mesto, matična številka, številka podjetja (mednarodna podjetja imajo izpostave tudi v tujini) itd. Sam kadrovski informacijski sistem ima lasten vmesnik za vzdrževanje podatkov. V Krki je kadrovski informacijski sistem razvit interno v podjetju, vendar je dolgoročni načrt selitev kadrovskih podatkov v SAP kadrovski sistem.

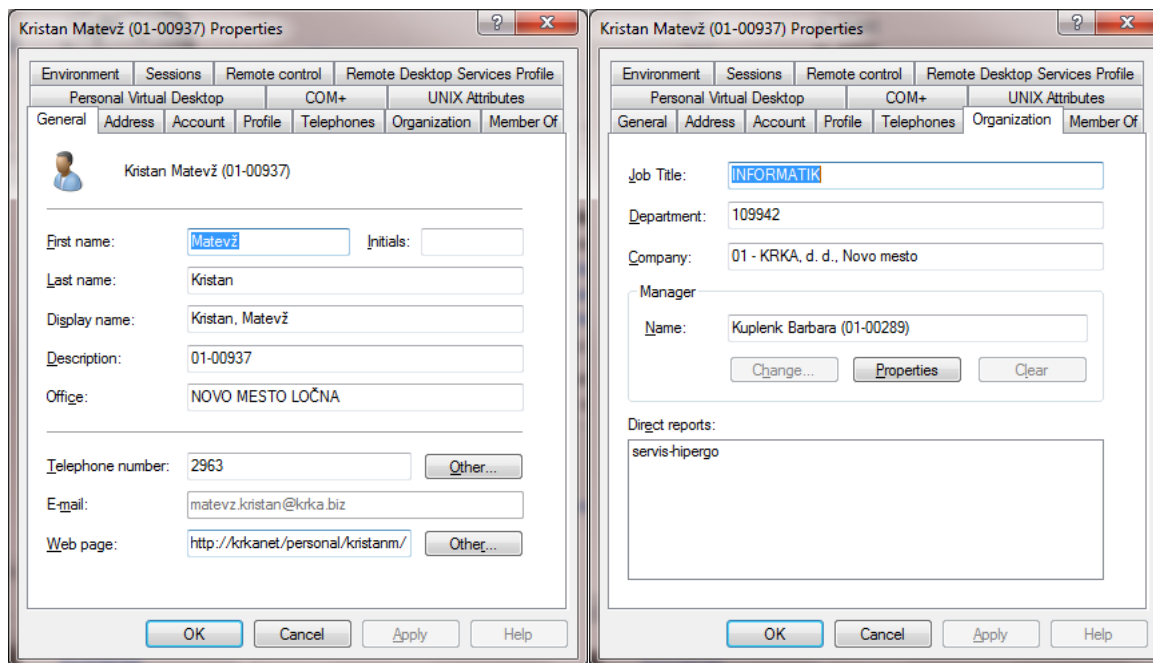
Imeniške storitve. Hramba podatkov o uporabniških imenih in geslih je danes pogosto izvedena kot imeniška storitev. V Krki uporabljamo (angl.) *Microsoft Active Directory*, ki je prvotno hranil zgolj uporabniško ime in geslo, naslov elektronske pošte ter pripadnost uporabniškega računa določeni skupini (AD skupine). Skozi razvoj podsistemov, ki uporabljajo aktivni imenik, smo v Krki postopoma več podatkov iz kadrovske baze in telefonskega imenika pričeli sinhronizirati skozi ročno izdelane skripte, ki so avtomatizirale prenos podatkov iz kadrovskega sistema v aktivni imenik. Danes je v Krki aktivni imenik centralna podatkovna baza, ki hrani »javne« podatke o zaposlenih – torej telefonske številke, delovna mesta, hierarhijo nadrejenih in podrejenih v smislu določitve odgovorne osebe (slika 3 prikazuje primer v Krki).

Sam aktivni imenik že omogoča razne storitve posodabljanja podatkov (ponastavitve in obnovitve gesla itd.). Aktivni imenik omogoča tudi »samopostrežbo«, v kolikor se definirajo pravice posameznim uporabnikom, da lahko določene podatke v aktivnem imeniku urejajo sami. Konfiguracija v Krki ne predvideva urejanja aktivnega imenika, saj se podatki v aktivni imenik črpajo iz drugih sistemov.

Elektronska pošta. Sistemi elektronske pošte so danes eni izmed najbolj razširjenih in uporabnih sistemov komuniciranja v vse modernejših podjetjih oziroma so nujni praktično za vsa podjetja, saj večina komunikacije, tako interne kot eksterne, poteka prek elektronske pošte. Sisteme elektronske pošte se pogosto kombinira tudi s **koledarskim sistemom** (ki je običajno sestavni del boljših poštnih strežnikov, kot na primer *Microsoft Exchange*, ki ga tudi uporabljamo v Krki), kar prinaša še določeno dodano vrednost samemu sporočilnemu sistemu (sklicevanje sestankov in dogodkov z uporabo opomnikov). Upravljanje uporabnikov elektronske pošte ima tudi lasten vmesnik za upravljanje. Posebnost *Microsoft Exchange* poštnega strežnika je v tem, da je povezan s sistemi aktivnega imenika. Tako

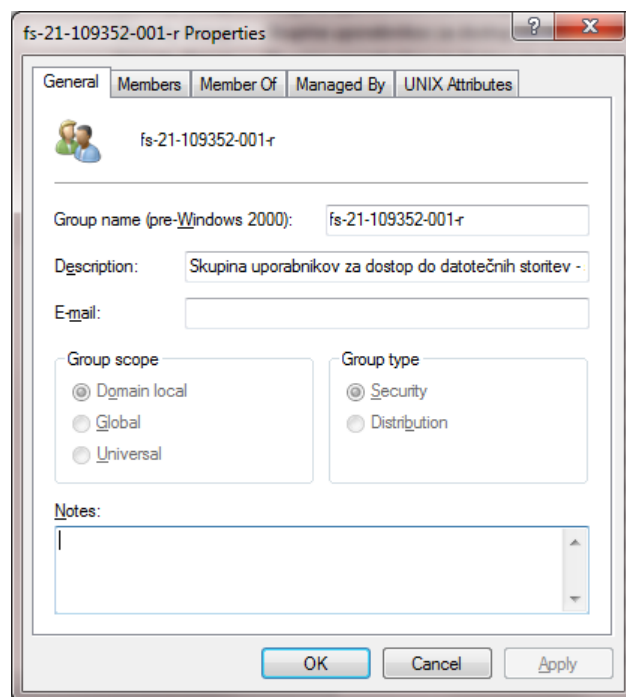
lahko definiramo proces avtomatskega kreiranja novega poštnega računa, vendar ponovno potrebujemo izdelavo skripte, ki unikatno določi elektronski poštni naslov.

Slika 3: Aktivni imenik in atributi uporabniškega računa



Datotečne storitve. Pogosta izmenjava datotek, predvsem večjih datotek in delovnih datotek, se je z distribucijo po elektronski pošti izkazala kot sila neučinkovita. Poštni strežniki so zaradi varčevanja s prostorom na diskih pogosto omejevali velikost tako sporočil kot tudi nabiralnikov, kar je uporabnikom predstavljalo nov izziv, kako uspešno izmenjevati in sodelovati na skupnih datotekah. Drug problem distribuiranja dokumenta preko elektronske pošte je »verzija« dokumenta pri pošiljanju. Večina računalniških omrežij omogoča takšno ali drugačno skupno rabo map, kjer hranimo datoteke (datotečne storitve). Ponovno nam v *Microsoft* okoljih priskoči na pomoč aktivni imenik. Vsak klient in strežnik ima vgrajeno datotečno storitev (angl. *File Sharing*), ki omogoča skupno rabo datotek. Običajna izvedba skupnih datotečnih storitev predvideva uporabo strežnika z veliko diskovno kapaciteto, ki se potem vsebinsko deli različnim skupinam uporabnikov. Upravljanje datotečnih storitev je pri velikem obsegu uporabnikov in števila skupnih map prava nočna mora, saj je zelo veliko relacij med uporabniki in skupnimi mapami, v ozadju pa potrebujemo še avtorizacije, da določeni uporabniki smejo uporabljati določeno storitev. Sama priporočila za upravljanje datotečnih storitev poudarjajo uporabo skupin iz aktivnega imenika – torej se pripadniki urejajo v skupinah AD (to je enotni vmesnik in gre za enako kot pri vzdrževanju uporabniških računov, slika 4), kar bistveno olajša administracijo – vendar še vedno ostaja problem ažurnega urejanja skupin (izločanje, premikanje, dodajanje uporabnikov je kontinuiran proces).

Slika 4: Urejanje skupin v AD



Tiskalniške storitve. Tiskalniške storitve so običajno upravljane lokalno, torej so tiskalniki nameščeni na osebne računalnike, ki jih lahko uporablja uporabnik določenega računalnika. V večjih oddelkih se zaradi zmanjšanja stroškov običajno namesti en skupni tiskalnik, katerega skrbnik tiskalniških storitev pripravi tako, da ga lahko uporabljajo samo zaposleni v takem oddelku. Pri velikih organizacijah, kot je Krka, je sistem tiskalniških storitev zelo kompleksen in povzroča podobne upravljaljske težave kot datotečne storitve.

Spletne storitve (Intranet, Ekstranet) in dokumentacijski sistemi. Z razvitostjo spletnih storitev, predvsem Intranet in Ekstranet portalov znotraj podjetja, se veliko delovnih tokov iz elektorskega poštnega sistema in sistema datotečnih storitev seli na Intranet (in/ali Ekstranet) portale. Prednost takih portalov, v primerjavi z datotečnimi storitvami, je v dodani vrednosti atributov, ki jih lahko pripnemo dokumentom (komu je namenjen, kdo je prvotni avtor, verzije ipd.) ter v primerjavi z elektronsko pošto (pri elektronski pošti je potrebno pošiljanje posodobljenih verzij dokumenta) ima prednost v tem, da lahko sistem sam obvešča naročnike o posodobitvah. Dolgoročno bodo sistemi spletnih storitev (pod kar vključujemo tudi Intranet in Ekstranet portale) v veliki meri izrinili datotečne storitve, saj v principu ponujajo osnovno datotečno storitev, ki je nadgrajena z dodatnimi možnostmi opisovanja samih datotek. Poleg tega ponujajo tudi vrsto novih storitev, kot so forumi, klepetalnice, ankete ipd. Vmesniki za upravljanje dostopov in uporabnikov so lastni različnim spletnim storitvam. V Krki je Intranet portal zgrajen z uporabo *Microsoft SharePoint Portal Server* tehnologijo, ki kot mnoge druge Microsoftove storitve uporablja aktivni imenik kot avtentikacijski sistem, vendar je samo upravljanje še vedno ločeno. Pri

uporabi skupin iz aktivnega imenika je upravljanje lahko podobno kot pri datotečnih storitvah z uporabo skupin.

Proizvodni informacijski sistem. Kot sem omenil že v poglavju 1.2, so proizvodni informacijski sistemi prisotni predvsem v večjih proizvodnih podjetjih. Krka v ta namen uporablja sistem nemškega proizvajalca Werum, ki se imenuje PAS-X. PAS-X je informacijski sistem za podporo farmacevtske proizvodnje. Je eden sodobnejših sistemov te vrste in je načrtovan tako, da upošteva posebnosti in zahtevnosti te specifične proizvodnje. Sistem zagotavlja spremljanje in nadzor celotnega dela farmacevtske proizvodnje z namenom zagotavljanja višjih standardov, kvalitete in zanesljivosti, ter zmanjšuje možnosti napak. Sistem ima razdelan lastni upravljavski modul, a nabor funkcionalnosti, ki jih ponuja Krkin proizvodni sistem, je preobsežen za potrebe te naloge, zato se ne bom spuščal v podrobni opis. Vključitev proizvodnega sistema v IdM sistem predstavlja velik izziv in bo vključen v IdM sistem verjetno kot zadnji sistem, predvsem zaradi svoje kompleksnosti.

Poslovni informacijski sistem. SAP R/3 je informacijski sistem poslovnih aplikacij, ki podjetjem omogoča informatizacijo poslovnih procesov, podprtih z naborom aplikacij. Ključna značilnost sistema je standardizacija in povezovanje številnih poslovnih procesov znotraj podjetja. Sistem se zelo dobro povezuje z različnimi okolji podjetja ter omogoča nemoten pretok podatkov med različnimi področji poslovanja – predvsem doprinaša enkratno ažuriranje podatkov skozi celotno podjetje, brez podvajanja vnosov ali sprememb. Sistem SAP R/3, ki ga uporabljamo v Krki, je namenjen podjetjem vseh velikosti, se pa pogosto v manjših podjetjih težko odločijo za nakup takega sistema, saj predstavlja izdatne stroške za manjša podjetja. Sistem ima lasten upravljavski modul, medtem ko podjetje SAP ponuja tudi lastno IdM rešitev, kot bom opisal v naslednjem poglavju. Torej poslovni informacijski sistemi (vsaj vodilni) so relativno dobro pripravljeni za integracijo v sistem upravljanja identitet.

Pristopna kontrola. Pristopna kontrola omogoča kontrolirano gibanje oseb po različnih objektih in lokacijah podjetja Krka in ureja posameznikov dostop do posameznih prostorov. Ključne naloge sistema pristopne kontrole so krajevno omejevanje vhodov in izhodov, časovno omejevanje vhodov in izhodov, evidentiranje in arhiviranje vsake registracije uporabnika, priprava različnih analiz in poročil iz arhivske podatkovne baze, alarmiranje posebnih stanj, ki se zgodijo znotraj sistema in interakcije na ostale sisteme tehničnega varovanja. Pristopna kontrola ima lasten upravljavski modul, ki je povezan s kadrovsko bazo samo preko unikatnega identifikatorja uporabnika, torej Krkine enotne matične številke.

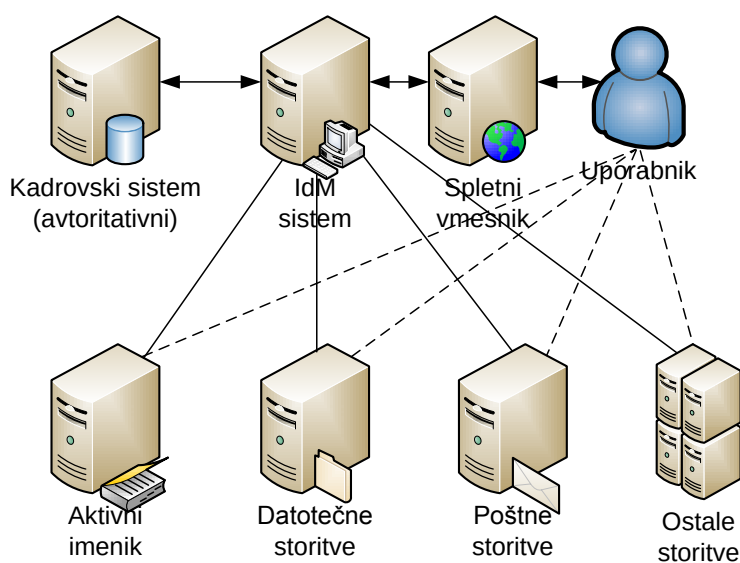
Poleg teh sistemov pa v podjetjih obstaja še mnogo manjših podsistemov, ki so bodisi bolj

ali manj razviti. Pogoj za učinkovito vključitev v sistem upravljanja identitet je zagotovo povezljivost takih sistemov z drugimi sistemi. Dober primer je poenostavitev upravljanja datotečnih storitev skozi AD skupine. Z uporabo AD skupin in sistemov, ki znajo uporabljati AD skupine, je vključitev upravljanja identitet relativno enostavna, v kolikor naš IdM sistem »zna« upravljati domenske (AD) skupine. Večina sistemov (oziroma praktično vsi IdM sistemi) znajo upravljati aktivni imenik, saj je aktivni imenik med najbolj razširjenimi sistemi v uporabi v modernih organizacijah.

2.2 Sistemi upravljanja identitet

Ker so si sistemi upravljanja identitet zelo podobni, tako po funkcionalnosti kot tudi po komponentah, ki jih sestavljajo, bom v tem poglavju predstavil najbolj tipično zgradbo sistema upravljanja identitet po komponentah. V naslednjem poglavju pa bom konkretne izdelke in ponudnike na trgu tudi predstavil.

Slika 5: Shema umestitve IdM sistema



Slika 5 prikazuje enostavno umestitev IdM sistema v okolje z nekaterimi tipičnimi storitvami. Črtkane črte na sliki predstavljajo poti prijave v sisteme, medtem ko polne črte predstavljajo upravljaljske poti – torej uporabnik se po eni strani prijavlja v sisteme s svojo **enotno prijavo**, po drugi strani pa preko spletnega vmesnika upravlja (kakršne so pač njegove pravice) IdM sistem in skozi njega tudi sisteme, povezane po upravljaljskih poteh. Dejanska izvedba v podjetju je navadno bistveno kompleksnejša – pomembno pa je, da imamo aktivni imenik, ki tudi skrbi za vse zahteve po avtorizacijah.

2.2.1 Komponente sistemov upravljanja identitet

Ključne komponente vsakega sistema upravljanja identitet so v osnovi štiri (Praprotnik, 2008, str. 32). Najpomembnejši, iz katerega izhajamo, je **imenik** (imeniške storitve) – običajno aktivni imenik, ki hrani podatke o digitalnih identitetah oziroma hrani podatke o samih uporabnikih. Sledi mu sistem za **upravljanje življenjskega cikla** (dodajanje, spreminjanje, brisanje in replikacija podatkov identitet). Tretji sistem je **sistem uveljavljanja in distribuiranja varnostnih politik** in izvajanje **avtentikacij ter avtorizacij**. Na zadnje mesto pa uvrščamo **sistem za poročanje** in izdelavo ter pregled revizijske sledi skozi celotni proces.

Celoviti sistemi upravljanja identitet ponujajo naslednje funkcionalnosti, ki so osnovne funkcionalnosti in jih mora vsak celovit sistem upravljanja identitet podpirati: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog uporabnikov, upravljanje dostopov do digitalnih virov, upravljanje (zveznih) identitet, sledenje, analiza in poročanje.

2.2.1.1 Imeniške storitve in imeniki

Vsak sistem, ki organizirano hrani določene podatke in uporabnikom nudi pregled teh podatkov in iskanje po njih, lahko uvrstimo v skupino digitalnih imenikov. Navadno taki imeniki omogočajo tudi urejanje teh podatkov v realnem času zato se jih je prijelo ime **aktivni imeniki** (angl. *Active Directory*), ki je tudi tržno ime najbolj razširjenega imenika v poslovnem svetu proizvajalca Microsoft, kot sem že omenil v prejšnjem poglavju (2.1.2)

V računalniškem svetu predstavlja imenik povezavo med imeni in vrednostmi, po katerih lahko poizvedujemo – zelo podobno kot telefonski imeniki ali slovarji. Povezave v imenikih so lahko bistveno bolj razvejane kot pa na primer pri telefonskem imeniku, čeprav ima že v telefonskem imeniku lahko ena oseba več telefonskih števil, kar nakazuje na več kot eno samo povezavo. Imeniki so lahko zelo skopi ali zelo bogati, tako po vsebini kot po naboru povezav med podatki (Hunter, Allen, 2008, pogl. 2, str. 1).

V Krki smo prvotno imeniške storitve uporabljali predvsem za kreiranje uporabniških računov zaposlenih in povezanih elektronskih poštnih naslovov. Danes pa je AD avtoritativni vir za marsikateri podatek, čeprav jih še vedno veliko samo prečrpava iz avtoritativnih virov, kot sta kadrovska baza in telefonski imenik.

Tehnično se uporabljata predvsem dva mrežna protokola za komunikacijo imenika z ostalimi imeniki (meta-imeniki) in uporabnikom. Prvotno je bil v uporabi predvsem

protokol X.500, ki je skupno ime za nabor več standardov, ki pokrivajo imeniške storitve. Razvit je bil v okviru združenj ITU⁶ in ISO⁷ v letu 1988 in sicer kot odgovor zahtevam standarda X.400 oziroma elektronski izmenjavi sporočil in imenskim poizvedbam. X.500 je poznan tudi kot »težki« protokol (Windley, 2005, pogl. 6.3, 9.3).

LDAP (ki sem ga omenil že v uvodnem poglavju) je danes najbolj razširjen protokol imeniških storitev in poznan tudi pod imenom »lahki« protokol. Predvsem so ga snovalci oblikovali tako, da poenostavlja določene funkcionalnosti težkega protokola (prvotno) z namenom prehoda na X.500, vendar se je zaradi svoje enostavnosti in prijaznosti do uporabnika (vključen je tudi uporabniški vmesnik) razvil v celovito imeniško storitev – ki je danes najbolj pogosto v uporabi v podjetjih po svetu (Windley, 2005, pogl. 9.3, str 1). LDAP vsebuje tudi metode za povezovanje na druge sisteme (tudi LDAP), ki nato delujejo skupno kot en imenik. Večina izvedb digitalnih imenikov predvideva replikacijo podatkov med posameznimi vozlišči imenikov – vendar standardi na tem področju niso urejeni (Windley, 2005, pogl. 9.3, 9.4). Vodilni produkti danes na trgu so: Active Directory – Microsoft, Open Directory – Apple, Oracle Internet Directory, Novell eDirectory itd.

Enotna prijava. Ideja v ozadju termina »enotna prijava« je v bistvu enkratna prijava uporabnika v sistem z enovito prijavo. Torej neka oseba, zaposlena v našem podjetju, prejme ob zaposlitvi podatke o svojem uporabniškem računu in geslo – z uporabo samo tega računa nato dostopa do raznih sistemov v podjetju. Tak način uporabe enotne prijave je danes zelo zaželen izvedba in hkrati kar nujna rešitev za IdM sisteme – saj IdM vsako identiteto prepozna kot unikatno in je tudi s tega stališča nujno, da se uporablja samo en način identifikacije uporabnika – z enotno prijavo, skozi vse sisteme (META Group, 2002, str. 7, 9). META Group in Windley ugotavljata, da se ob uporabi enotne prijave število klicev v oddelek za pomoč uporabnikom zmanjša za eno tretjino in prav za toliko se tudi poveča stopnja varnosti. Predvsem pa je ključni efekt enotne prijave uporabniška izkušnja – ena poverilnica za vse sisteme (Windley, 2005, pogl. 9, 11, 12, 13).

Združevanje podatkov in zvrsti imenikov. Kljub razširjenosti aktivnih imenikov in uporabe enotne prijave vsi programi in sistemi ne podpirajo tehnologije, kar je mogoče zaradi zastarelosti ali zgolj neupoštevanja standardov na področju programske opreme. Rešitev za vključitev takih sistemov v upravljanje identitet poteka skozi fazo združevanja podatkov, ki je lahko izvedena v naslednjih oblikah:

- centralna podatkovna baza,
- meta-imeniki, ki sinhronizirajo podatke različnih podatkovnih baz,
- virtualni imeniki, ki ponujajo poglede na različne imenike skozi enoten vmesnik,

6 ITU je kratica za International Telecommunication Union

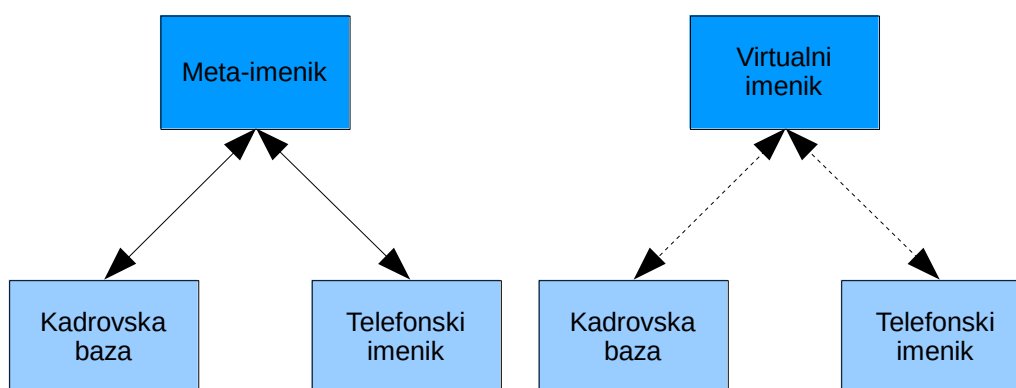
7 ISO je kratica za International Organization for Standardization

- federativni (ali zvezni) imeniki, ki povezujejo podatkovne baze.

Če si pogloblje in na kratko ogledamo posamezne zvrsti imenikov, bomo hitro ugotovili zakaj so t. i. meta-imeniki danes najbolj razširjeni v praksi. **Centralna hramba podatkov** je sicer najbolj enostavna izvedba, saj predvideva vse podatke v eni sami podatkovni bazi. Enostavnost take baze pa na drugi strani pomeni spremembo sistemov, da bodo uporabljali to enotno podatkovno bazo. Sami vemo, da so posegi v določene sisteme praktično nemogoči ali včasih stroškovno nesprejemljivi, zato poznamo še druge tipe hrambe podatkov, ki predvidevajo razpršene vire podatkov.

Ideja **meta-imenikov** je zbiranje podatkov iz več različnih imenikov in prikaz uporabniku kot enotni imenik. Tipično imajo podjetja danes podatke shranjene v več imenikih, ki jih nato povezujejo v meta-imenike za potrebe upravljanja identitet. Prednost takega združevanja podatkov se kaže tudi v možnosti selekcije tipa podatkov iz posameznega imenika – torej ne združujemo vseh podatkov iz imenikov, temveč samo tiste, ki jih dejansko potrebujemo. Meta-imeniki podatke **sinhronizirajo** v lastno podatkovno bazo – zato podatki niso »živi«, ampak posodobljeni z neko časovno zamudo.

Slika 6: Primer meta-imenika in virtualnega imenika



Na sliki 6 vidimo dvosmerno komunikacijo med imeniki in meta-imenikom oziroma virtualnim imenikom. Česar pa ne vidimo na sliki, je segregacija podatkov, ki jih sinhroniziramo – torej ne vseh, vendar samo potrebne. Črtkane črte pri virtualnih imenikih predstavljajo samo navidezne povezave – poizvedbe v realnem času, medtem ko pri meta-imenikih podatke po povezavah sinhroniziramo.

Podobno kot meta-imeniki se obnašajo tudi **virtualni imeniki**. Na videz so virtualni imeniki podobni meta-imenikom, razlikujejo pa se v lastni bazi podatkov. Virtualni imeniki namreč nimajo lastne baze podatkov, temveč ponujajo samo pogled na različne podatkovne vire (baze) z izvajanjem poizvedb v realnem času. Prednost takih imenikov je torej v sposobnosti prikazovanja podatkov, ki se pogosto spreminjajo in je sinhronizacija pri meta-

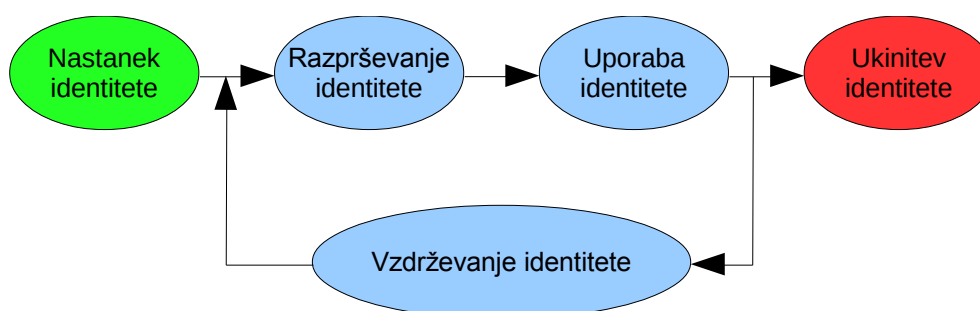
imenikih dejansko ovira. Ta problem uspešno rešujemo z virtualnimi imeniki.

Še ena izvedba povezanih imenikov so **federativne identitete** ali zvezne identitete, kjer podatke ponovno hranimo v bazah avtoritativnih virov, sistem federativnih identitet pa ustvari povezave z mehanizmom na višjem nivoju, ki opredeljuje relacijo med posameznimi podatki v različnih imenikih. Federativne identitete so pogosta oblika izvedbe pri sistemih upravljanja identitet, medtem ko so meta-imeniki pogosta rešitev, kadar imenike sinhroniziramo (Windley, 2005, pogl. 12, str. 1; Reed, 2002, str. 67).

2.2.1.2 Življenjski cikel identitet

Za vsak živ sistem lahko rečemo, da imajo entitete tega sistema življenjski cikel in tudi sistem sam ima življenjski cikel. Poznavanje življenjskega cikla identitete je ključnega pomena za razumevanje vpeljevanja sistema upravljanja identitet. Življenjski cikel identitete lahko ponazorimo s sliko 7 (Windley, 2005, pogl. 5), ki opredeljuje 5 življenjskih faz identitete in sicer nastanek, razprševanje, uporabo, vzdrževanje in ukinitvev identitete:

Slika 7: Življenjski cikel identitete



Nastanek identitete ali angl. *Provisioning* je začetek novega življenjskega cikla, ki je v primeru digitalnih identitet realiziran kot zapis v določeni bazi podatkov. Za lažjo predstavbo bom vsak korak opisal na primeru uporabnika. Torej nastanek identitete je prvi zapis v podatkovni bazi, ki ustvari identiteto uporabnika s pripadajočimi potrebnimi podatki (na primer ime, priimek, naslov itd.). Predvsem pomembna s stališča upravljanja identitet je v prvem koraku zagotovitev ustvarjanja identitet v vseh sistemih, ki jih uporabnik potrebuje za svoje delo – to pa predstavlja naloge več skrbnikov in posledično daljše čakalne dobe. IdM sistemi s procesom definirajo nastanek identitete in nato še **razprševanje identitete** v podrejene sisteme, kar tipično skrajša čas ustvarjanja identitete, saj skrbniki nimajo več nalog, saj le-te izvede sistem, vpis nove identitete pa se prenese na osebo, ki je dejansko odgovorna za prave podatke – lahko v obliki samopostrežbe. Razprševanje identitete je seveda potrebno samo tam, kjer imamo več avtoritativnih virov podatkov, več imenikov itd. **Uporaba identitete** je nato v domeni uporabnika samega, ki

jo uporablja pri svojem delu in je s stališča upravljanja identitet to najbolj enostavna faza. **Vzdrževanje identitete** skozi njen življenjski cikel je ključno za vse žive sisteme. Posamezni atributi identitete se spreminjajo in potreben je mehanizem za posodabljanje teh podatkov. Kot omenja Windley je razlogov za spremembo atributov veliko, saj lahko izvirajo iz poslovnih priložnosti ali pa nastajajo novi atributi z dodajanjem novih sistemov. Pomembno je, da se spremenjeni podatki prenesejo na vse povezane sisteme (avtomatsko ali ročno). Vzdrževanje velikega števila identitet v enem samem oddelku (pomoč uporabnikom, kot je to običajno) je zelo kompleksno in časovno potratno, zato sistemi omogočajo tudi delno samovzdrževanje identitet – torej imajo uporabniki možnost spreminjanja določenih podatkov o svoji identiteti, imajo možnost samostojne menjave gesel ipd., kar bistveno razbremeni oddelke za pomoč uporabnikom, (Windley, 2005, pogl. 5, str 4). **Ukinitev identitete** je prav tako pomembna kot ustvarjanje identitete. Preden nekemu zaposlenemu ne ustvarimo identitete in pripadajočih pravic na sistemih, ne more delati. Ko pa se določen zaposleni upokoji ali zapusti podjetje, pa je ključnega pomena za varnost podatkov podjetja, da se mu ukine identiteto in/ali tej identiteti ukine dostopne pravice na sistemih. V kolikor se identitet ne ukine pravočasno oziroma se jim ne odvzame dostopov do sistemov, je to lahko veliko tveganje za podjetje (Windley, 2005, pogl. 5).

2.2.1.3 Varnostni mehanizmi in upravljanje dostopov ter overitev

V prvih dveh podpoglavjih sem torej opisal imeniške storitve kot vir in hrambo podatkov (bodisi centralizirano ali razpršeno) ter življenjski cikel posamezne identitete. Sama uporaba identitete v nekem digitalnem okolju pa zahteva tudi sisteme za overitev identitet ter sisteme vlog in pravilnikov, ki na določenih sistemih nastavljajo ustrezne pravice identitetam.

Overitev je proces, ki preveri identiteto uporabnika, ki želi dostopati do izbranih vsebin z uporabo svoje poverilnice (na primer uporabniško ime in geslo). V kolikor obstaja povezava med njegovo identiteto in sistemom preko **vloge** na sistemu, se uporabniku v tem okviru dovoli dostop, sicer ne. Overitev je proces preverjanja oziroma odločanja o tem, kaj nekdo je in za kaj se izdaja (Rouse, 2007, *Authenitication Definitions*).

Običajno se torej uporablja uporabniško ime in geslo za dostope do računalniških sistemov, za dostope v fizične prostore pa pogosto identifikacijske kartice in pristopna kontrola. Oboje spada v nabor t. i. *poverilnic* identitete, ki so lahko še biometrične (na primer prstni odtis) ali kombinacija vseh treh – torej kaj vemo, kaj imamo in kaj smo.

Upravljanje gesel je namreč nujno ob vsaki uporabi takih poverilnic, saj so uporabniška gesla in imena enostaven način uporabe s primerno varnostjo. Seveda so prisotne tudi težave, ki jih rešujemo z upravljanjem gesel (na primer ponastavitve pozabljenega gesla

uporabniku, obvezna menjava gesla v določenem obdobju itd.). Oddelek za pomoč uporabnikom mora v primeru menjave gesla uporabniku vzpostaviti neko mero zaupanja do uporabnika, da mu lahko ponastavi geslo. V Krki je na primer potrebno odgovoriti na niz vprašanj (interna telefonska številka zaposlenega, matična številka zaposlenega ipd.) ter še nekaj zelo pomembnega: v primeru telefonskega klica mora biti le-ta opravljen iz internega Krkinega telefona ali mobitela, kar se da preveriti v internem telefonskem imeniku. Drugi podoben primer pa je sprememba lastnega gesla po preteku življenjske dobe gesla, ki je nekje 90 dni. Ker bi menjava gesel preko oddelka za pomoč uporabnikom ustvarila veliko nepotrebnega dela tam zaposlenim, je zelo smiselno vpeljati sistem za samozamenjavo gesla, poleg tega pa se prvotno opisano »pozabljeno« geslo ravno tako poveže s tem sistemom preko pravil – na primer uporabnik odgovori na niz zastavljenih vprašanj in v kolikor se odgovori ujemajo s podatki v kadrovske bazi, si uporabnik lahko sam zamenja geslo.

Ves čas torej govorim o samo **enem** geslu in uporabniškem imenu, saj predpostavljam, da uporabljamo **enotno prijavo** (SSO). To je mehanizem preverjanja poverilnic na različnih sistemih, vendar iz enega samega sistema poverilnic. Najlažje si predstavljamo prijavo v osebni računalnik z uporabo domene – torej skupine ljudi in naprav, ki so povezane preko enotnega imenika in mehanizmov preverjanja. Takšen način omogoča SSO prijavo na vseh napravah povezanih v domeno. Sistem je dokaj dobro razvit za Microsoftove produkte in tudi za niz produktov ostalih ponudnikov, ki znajo uporabljati Windows način avtentikacije in domenskih prijav – kar že samo po sebi precej olajša upravljanje uporabnikov znotraj domen.

Slika 8: Prijavno okno: uporabnik, geslo, domena (levo), na desni brez domene



Odločitev o uvedbi enotne prijave je zelo strateška, saj po eni strani omogoča udobje dela, lažjo administracijo centralno zbranih uporabnikov, a po drugi strani prinaša tudi večje tveganje, saj zloraba enega uporabniškega imena pomeni dostop do vseh sistemov, vezanih na ta račun. Na sliki 8 lahko vidimo, kako malo se razlikuje prijava lokalno od domenske

(vizualno) v ozadju pa je vzpostavljen mehanizem preverjanja domenskega gesla preko aktivnega imenika.

2.2.1.4 Sistemi revizije in poročanja

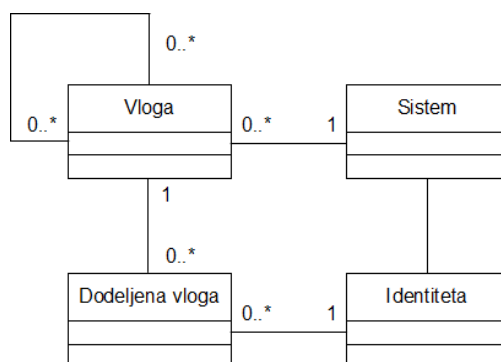
Sistemi upravljanja identitet so lahko sicer zelo enostavni, a pogosto raje kompleksni, ker se povezujejo na mnogo različnih sistemov in vsak sistem zahteva posebna pravila pri povezovanju. Tu definiramo preslikave povezav iz IdM sistema proti povezanemu sistemu (na primer kako se preslika podatek »ime« iz kadrovske baze v IdM sistem). Z uporabo orodja za upravljanje z identitetami si moramo zagotoviti tako upravljanje kot tudi sledenje identitetam skozi njihov celoten življenjski cikel. Življenjski cikel identitet lahko navadno prilagajamo našim potrebam, saj so delovni tokovi nastavljivi in prilagodljivi posameznim poslovanjem – vsem sistemom pa je skupen način poročanja in sama sposobnost sledenja spremembam. **Sistem poročanja** (angl. *Reporting services*) naj bi bil zasnovan tako, da omogoča **popolno revizijsko sled**, kar pomeni, da obstaja zapis o vsaki spremembi identitete: kdo je spreminjal kateri podatek, kdaj in kje ipd. Posledično se lahko ustvari poročilo o spremembah na določeni identiteti. Sistemi torej ponujajo tako poročila kot vrtanje (**sledljivost**) posamezne izbrane identitete, vloge itd. Poleg tega sistemi poročanja omogočajo razne poglede, kot so: kdo ima dostop do izbranega sistema, kdo ima dostop do izbranega resursa itd.

2.2.2 Entitete sistemov upravljanja identitet

Da bi lahko uspešno identificirali osnovne entitete sistemov upravljanja identitet, bomo kot osnovni entiteti definirali **sistem** in **identiteto**, ki predstavljata tako uporabnika kot področje dela (sistem). Vsak sistem pa vsebuje tudi **vloge**, ki opredeljujejo, kaj lahko določena oseba na sistemu počne in analogno imajo tudi identitete (na primer zaposleni) pripadajoč objekt **dodeljene vloge**, ki povezuje vloge na sistemih z identitetami. Za boljšo predstavbo, si lahko pomagamo z meta- modelom, ki opisuje povezave med entitetami (slika 9).

Vsakemu sistemu torej pripada ena ali več vlog in vsaka vloga je lahko dodeljena eni ali več identitetam. V meta-modelu nastopa identiteti dodeljena vloga kot vezna entiteta med vlogami in identitetami, to pa ni nujno vedno tako – rešitev je izvedena kot dodaten atribut v sami vlogi, ki dovoljuje več zapisov – v takem primeru bi imeli potem v meta-modelu 3 entitete. Za potrebe razumevanja entitet zgornja slika predstavlja enostaven sistem upravljanja identitet.

Slika 9: Entitete



2.2.2.1 Identiteta

V filozofiji je identiteta definirana kot »enakost« (kar pomeni tudi prevod latinske besede *identitas*) in sicer enakost vseh atributov. Leibnizov zakon pa pravi za vsako stvar, ki ima popolnoma enake lastnosti kot neka druga stvar, da to ni le njena kopija, temveč je to popolnoma enaka stvar. Koncept enakosti je ustvarilo tako osebni kot socialni pomen identitetam kot enoličnim entitetam.

Vsaka entiteta je lahko le popolnoma enaka sebi, kakršnakoli razlika pa že privede do nove identitete. Tako je torej identiteta v bistvu nabor lastnosti in karakteristik, ki razlikujejo izbrano entiteto od ostalih entitet enolično (Bowie, 1993, str. 55-57).

Leta 1974 je Salvador Minuchin ugotovil, da ima identiteta za človeka dva pomena – pomen pripadnosti in samostojnosti (ali ločenosti). Ta opis pa zelo sovпада z današnjim pojmovanjem **digitalne identitete**. Digitalna identiteta v prvi vrsti enolično opisuje neko osebo ali stvar, po drugi strani pa ta oseba ali stvar tudi opiše relacije z drugimi entitetami – kar pa je točno to, kar nam prikazuje zgornja slika. Poleg tega pa lahko ločimo digitalne subjekte na človeške (osebe) in nečloveške (naprave, viri, pravila itd.) (Windley, 2005, pogl. 2).

2.2.2.2 Sistem

Najpomembnejše sisteme za upravljanje identitet sem že opisal v poglavju 2.1.2. V grobem pa sam sistem za nas predstavlja običajno informacijski sistem ali storitev, ki je del organizacije ali pa celo izven organizacije. Sistemi se za podjetja ločijo še po pomembnosti, nekateri so nujni za poslovanje podjetja (angl. *Business-critical*), drugi

manj. Ti sistemi postanejo zanimivi za naše opazovanje šele takrat, ko jih povežemo z IdM sistemi, kar pa je tudi bistvo vpeljave samega IdM sistema. Najbolj tipični sistemi, ki jih povezujemo najprej, so: kadrovski informacijski sistem, uporabniki v aktivnem imeniku, elektronska pošta in urejanje skupin v aktivnem imeniku.

2.2.2.3 Vloga

Vloga predstavlja niz lastnosti, ki omogočajo dostop do sistema, dostop do storitve sistema ali samo storitev sistema (pravica, dostop, programska in strojna oprema, poštni predal, distribucijska skupina itd.) Pod pomenom vloge se lahko skriva veliko različnih stvari, torej se vloge ločijo tudi po tipu. Več kot imamo sistemov povezanih v IdM sistem, več imamo različnih vlog – saj vsak sistem vključi v IdM svoje vloge. Ker pa IdM sistemi nudijo enoten pogled na vse vloge v IdM sistemu, posledično tako pridobimo bistveno boljšo preglednost nad posameznimi vlogami in tipi (na primer pravice, dostopi itd.).

2.2.2.4 Dodeljevanje vlog

Dodeljevanje vlog pa je logično povezovanje samih identitet in vlog. Ta tip entitete je zelo preprost, saj vsebuje samo kazalnik na vlogo in identiteto. Navadno pa vsebuje še nekaj podatkov, ki odražajo življenjsko dobo dodeljene vloge in po potrebi dodatne opisne attribute.

Tabela 2: Dodeljevanje vlog in tipi

Identite ta	Sistem	Vloga	Dodeljen:
Matevž Kristan	Aktivni imenik	Dostop	Uporabniški račun
or123456si	Aktivni imenik	Dostop	Računalniški račun
Matevž Kristan	Elektronska pošta	Poštni predal	Poštni račun

V primeru, ki ga prikazuje tabela 2, je polje »Dodeljen:« predstavljeno kot rezultat ustvarjen v sistemu – torej posledica dodeljevanja vloge. Tak način, kot ga predstavlja tabela, sovпада s predstavitvijo entitet v poglavju 2.2.2, lahko pa bi bilo dodeljevanje vlog izvedeno tudi kako drugače.

2.3 Predstavitev in analiza sistemov za upravljanje identitet

Da bi lahko učinkovito preučili izdelke na trgu, je potrebno najprej razumeti, kaj točno podjetje potrebuje od končnega izdelka. Sama tehnična dovršenost še ne pomeni tudi najlažjega življenja s takim sistemom, saj lahko izbira različnih dobaviteljev ključno vpliva

na odločitev o izbiri sistema. Cilj tega poglavja je predstaviti najprej dejavnike in karakteristike izbora sistemov, nato predstaviti vodilne ponudnike rešitev in na koncu pripraviti analizo po določenih kriterijih med izbranimi ponudniki rešitev.

2.3.1 Dejavniki in karakteristike izbora sistemov

Pri izbiri ponudnikov IdM sistemov in samih IdM sistemov (produktov) za podjetje stopata v ospredje dva ključna dejavnika: prisotnost določenega sistema in zanesljivega ponudnika na dostopnem (običajno domačem, ni pa nujno) trgu ter skladnost funkcionalnosti, ki jih izbrani sistem nudi, glede na posamezne razpršene podsisteme v podjetju. Predvsem v večjih podjetjih, kjer imajo vpeljane svetovno razširjene sisteme, kot so na primer SAP ali Oracle sistemi, je izbira glede funkcionalnosti lažja, saj večina vodilnih ponudnikov IdM rešitev že ponuja povezovalne module (agente), ki omogočajo izmenjavo (sinhronizacijo) podatkov med sistemi in IdM sistemom (Bisaerts, 2011, *Top 5 Identity management vendors of today*).

Določitev samih tehničnih lastnosti rešitve, ki jo potrebujemo, izvira specifično iz samega podjetja, torej iz sistemov, ki jih že uporablja. Hkrati pa ima podjetje tudi že dobavitelje teh sistemov ter z njimi bodisi boljše ali slabše izkušnje, kar lahko vpliva na odločitev o izbiri novih sistemov, ki jih morda ponuja dobavitelj. Pomen *dobrega* dobavitelja za podjetje je lahko različen, vendar v splošnem predstavlja kompetentno podjetje, ki svoje obveznosti vrši dovolj hitro glede na zahteve kupca in nudi kupcu kvalitetne dobrine. Da bi lahko podjetje še lažje identificiralo dobre lastnosti rešitev, ki jih dobavitelji ponujajo, si lahko pomagamo s priporočili skupine Gartner. Kasneje je potrebno sam izbor med rešitvami dopolniti še z lokalno ponudbo dobaviteljev IdM rešitev. Skupina Gartner definira nekaj karakteristik, ki opredeljujejo vodilne proizvajalce IdM sistemov:

- Na prvem mestu mora proizvajalec sistema imeti predvsem sposobnost dobre vpeljave svoje rešitve, bodisi v lastni režiji ali s partnerji. Imeti mora močno razvejana partnerstva po svetu in sposobne partnerje, ki vpeljujejo rešitve in so ključnega pomena za uspešnost izbrane rešitve, prav tako reference in prisotnost na več trgih povečujejo ugled rešitve.
- Dobro projektno vodenje, definiranje jasnih korakov in ciljev, opravljena podrobna analiza sistemov in pripravljen podroben načrt rešitve ter tudi realni časovni roki vpeljave sistema (bodisi posameznih faz s strategijo nadaljnjega razvoja).
- Modularnost izdelka, ki ponuja kupcu nakup samo tistih modulov, ki jih dejansko potrebuje za svojo rešitev in ne po nepotrebnem celotnega izdelka z vsemi moduli.
- Razširljivost in nastavljivost dobrega sistema omogočata vpeljavo enotnega produkta v več različnih rešitev. Medtem ko slabši ponudniki prilagajajo sam produkt, dober proizvajalec samo prilagodi nastavitve svojega.

- Dobra lastnost kvalitetne rešitve leži tudi v pripravljenih postopkih za migracijo iz konkurenčnih rešitev ter postopkih nadgradnje in razširljivosti sistema.
- Skrb za stranko po vpeljavi sistema je tudi nujna za dolgoročno uspešnost rešitev. Bodisi nove stranke ali stranke, ki so zamenjale en IdM sistem za drug, potrebujejo kar nekaj časa, da se na nove rešitve privadijo in jih pogosto še malenkostno prilagajajo. Slaba podpora dobavitelja v tem segmentu lahko ključno vpliva na uspešnost rešitev.

Zgornje karakteristike opisujejo kriterije ocenjevanja skupine Gartner za izdelavo t. i. magičnega kvadranta najboljših igralcev (ponudnikov) rešitev upravljanja identitet, kar pa še ne pomeni, da je vodilna rešitev tudi najboljša za naše potrebe, nam pa predstavi kar nekaj ponudnikov na tem področju.

Vodilni ponudniki torej niso nujno najboljši za vsako rešitev in imajo lahko višje skupne stroške kot pa ne-vodilni ponudniki. Prednost vodilnih pa je pogosto v manjšem tveganju vpeljave in boljši integraciji z lastnimi in konkurenčnimi sistemi. Po mnenju skupine Gartner so vodilni igralci tudi poštena in verodostojna podjetja, ki jim je moč zaupati.

2.3.2 Vodilni ponudniki rešitev

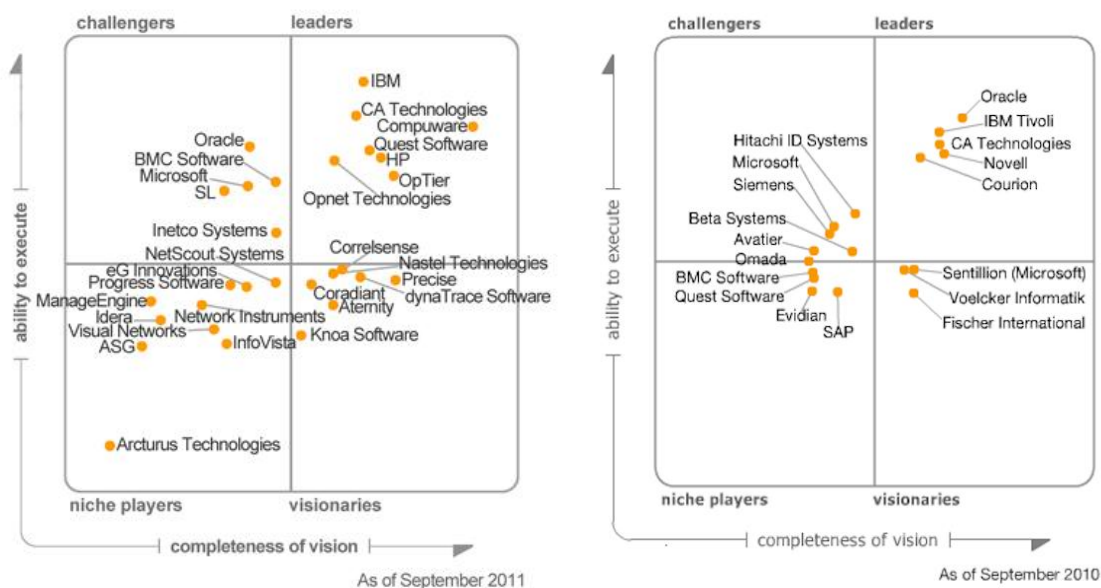
Vodilni ponudniki IdM rešitev v svetu (Gartner 2010) so predstavljeni v magičnem kvadrantu skupine Gartner za leto 2010 (slika 10), kjer izstopa 5 ponudnikov v kvadrantu vodilnih in ki hkrati predstavljajo obdobje, v katerem smo pripravljali izbor med ponudniki v podjetju Krka:

1. Oracle,
2. IBM Tivoli,
3. Computer Associates (CA),
4. Novell,
5. Courion.

Zanimivi igralci (izzivalci) pa so še Hitachi ID Systems in Microsoft, Siemens, Beta Systems, Avatier in Omada (ki svoje rešitve temeljijo na souporabi Microsoftovega sinhronizacijskega servisa).

Za primerjavo dodajam novejšo sliko iz septembra 2011, kjer lahko opazimo napredek podjetij IBM in Microsoft, izgubila pa sta se SAP in Novell. Poleg starih igralcev pa je na področju zacvetelo mnogo novih, ki bi zaslužilo preučevanja, vendar bi to preseglo obseg te naloge, zato sem v ospredje vzel igralce, ki so bili najpomembnejši v času izbora ponudnika v podjetju Krka, d. d. Sam postopek izbire pa je univerzalen in se lahko uporabi za nadaljnje preučevanje ostalih ponudnikov.

Slika 10: Vodilni ponudniki IdM rešitev 2010 in 2011



Vir: Gartner's Magic Quadrant for Identity Management

2.3.2.1 Oracle (vključno s podjetjem Sun)

Oracle je po letu 2006 prevzel vodstvo v magičnem kvadrantu, saj je svojo rešitev Oracle IAM zelo izpopolnil, dodal mnogo novih funkcionalnosti ter tudi nanizal vrsto uspešnih vpeljav v velika mednarodna podjetja. V zadnjem letu, ko je Oracle kupil podjetje Sun, pa je dosegel še dve ključni prednosti: odstranitev enega konkurenta ter še bolj pomembno za samo IdM rešitev je dejstvo, da so vpeljali vpogled in dostop do mnogih rešitev podjetja Sun (na primer *Sun Role Management*, ki je zdaj poznan kot *Oracle Identity Analytics*).

Oracle je predan dobavi obsežnega in kvalitetnega IdM sistema. Čeprav v zadnji raziskavi Gartnerja še ni vključena najnovejša različica 11g, ki pa (če gre verjeti obljubam dobavitelja) zagotavlja nadaljnje vodstvo Oracla v prihodnjih letih.

Tehnično Oracle IAM podpira veliko raznovrstnosti, saj poteka na kar sedmih različnih operacijskih sistemih, dveh vodilnih podatkovnih bazah in štirih različnih aplikacijskih strežnikih. Poleg tega Oracle pridobiva nove modularne rešitve tudi z nakupi podjetij, ki jih razvijajo, in jih vključuje v svojo rešitev ter vzdržuje in nenehno povečuje svoja partnerstva po svetu.

Oracle IAM ponuja: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do digitalnih virov, upravljanje zveznih

identitet, sledenje, analizo in poročanje. Ponuja spletne uporabniške vmesnike, ki so enostavni in uporabniku prijazni.

2.3.2.2 IBM Tivoli

IBM Tivoli je že dobro desetletje prisoten na tržišču kot vodilni ponudnik rešitev upravljanja identitet. Podjetje nosi že stoletno tradicijo in mu samo prestižno ime odpre marsikatera vrata pri sklepanju poslov. Vendar jih samo to dejstvo ne drži v vodilnem kvadrantu. IBM ima partnerstva širom po svetu in tudi veliko lokalnih izpostav (na primer IBM Slovenija), ki skrbijo za uspešne vpeljave IBM Tivoli Identity Management sistemov. Čeprav je v zadnjem letu sam razvoj produkta nekoliko zamrl, pa gredo zasluge zato predvsem k prestrukturiranju trga, ki zahteva čedalje večjo skladnost s standardi in preusmeritev fokusa iz administracije v skladnost pri samem razvoju produkta. Vodstvo podjetja je to rešilo tako, da svojim strankam ponuja zgodnji vpogled in sodelovanje pri izdelavi zadnje verzije.

Prav tako kot Oracle deluje IBM Tivoli na vrsti operacijskih sistemov, baz in aplikacijskih strežnikih ter ponuja upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do digitalnih virov, upravljanje zveznih identitet, sledenje, analize in poročanje. Poleg tega pa ponuja simulacijo vseh pravil pred vključitvijo v delovno okolje.

2.3.2.3 Computer Associates (CA)

Podjetje *CA Technologies* je znano po agresivnem trženju, prodaji ter po agresivni strategiji integracije. Večje povezovanje z mednarodnimi podjetji in posvetovanja so ključni pri prodaji njihovega sistema *CA Identity Manager*. Tudi CA je na trgu prisoten več kot desetletje in kot tak dokazuje sposobnosti in karakteristike, ki ga uvrščajo med vodilne igralce na področju IdM. Podobno kot Oracle tudi CA veliko modulov realizira z nakupom manjših podjetij.

Poleg prisotnosti na trgu pa je CA intenzivno prisoten pri pisanju standardov iz področja upravljanja identitet. Podpirajo tako tehnične standarde (na primer SMPL) kot tudi standarde iz upravljanja storitev in smernic IT poslovanja (ITIL).

Po oceni skupine Gartner je CA v zadnjih najbolj napredoval v kvadrantu vodilnih igralcev. Tako kot ostali sistemi tudi *CA Identity Manager* podpira: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do

digitalnih virov, upravljanje zveznih identitet, sledenje, analizo in poročanje.

2.3.2.4 Novell

Novell počasi a vztrajno izboljšuje svoj položaj med vodilnimi ponudniki rešitev za upravljanje identitet predvsem s partnerstvi ter intenzivnim trženjem in prodajo. Nizi izdelkov, ki jih ponujajo, so realizirani kot en homogen proizvod, saj je skoraj v celoti nastal v samem podjetju (brez prevzemov in nakupov drugih podjetij), kar uporabnikom predstavlja zelo enovito rešitev. Prav tako veliko tehničnih strokovnjakov ocenjuje Novellovo rešitev kot tehnično odlično ter usmerjeno v prihodnost (vizionarsko), saj Novellova strategija že danes ponuja tudi rešitve v oblaku (angl. *Cloud-based Solutions*), kjer gre torej za upravljanje identitet kot storitev za podjetja brez nakupa in vzdrževanja lastne opreme. Na tem mestu bi omenil partnerstvo s podjetjem Vmware, ki je vodilno podjetje v svetu virtualizacijskih tehnologij, kar Novellu daje še dodatno prednost in inovativnost na tem področju.

Gartnerjeva raziskava za leto 2010 je odkrila še zanimivo posebnost pri prevzemu Suna s strani Oracla. Gre za to, da so se nezadovoljne stranke obračale predvsem k rešitvam Novella. Sun je bil večinski sponzor mnogih odprtokodnih projektov, ostra Oracle politika pa je zamajala temelje več takih projektov in posledično tudi zaupanje strank do Oracla.

Novellove rešitve ponujajo: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do digitalnih virov, upravljanje zveznih identitet, sledenje, analizo in poročanje. Ponujajo tudi zelo izpopolnjene spletne uporabniške vmesnike, ki so enostavni in uporabniku prijazni – enovita izkušnja skozi vse module.

2.3.2.5 Courion

Courion je edino podjetje med najboljšimi petimi, ki se izključno ukvarja z izdelavo sistemov upravljanja identitet in mu pravijo tudi edini *pure-play* igralec. Courion ohranja in postopoma povečuje svojo prisotnost v vodilnem kvadrantu predvsem zaradi izboljšanja tržne strategije in inovacij. Prav tako so že v letu 2008 pričeli z razširitvijo portfelja in tako ponujajo sedaj vse module upravljanja identitet (dodane so še analiza, revizija in poročanje). Njihov glavni cilj je v poenostavitvi uporabe in izdelavi kar čim bolj poslovno prijaznega izdelka.

Kljub temu, da je večina Courion strank oziroma podjetij manjših (glede na svetovne

razmere), pa je njihova rešitev prav tako uspešno uvedena v nekaj izjemno velikih okolij, ki imajo preko milijon uporabnikov – kar daje podjetju zelo kredibilne reference. Prav tako kot ostali tudi Courion nenehno sklepa in vzdržuje partnerska razmerja – najbolj odmevna imena sta RSA (upravljanje dostopov) in Citrix (*XenApp provisioning*, dodeljevanje pravic). Dodatno nudijo nekaj funkcionalnosti, ki jih ostali konkurenti ne ponujajo, na primer integrirano zaščito pred izgubo podatkov, upravljanje uporabniških aktivnosti itd.

Courion Access Assurance Suite podpira: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do digitalnih virov, upravljanje zveznih identitet, sledenje, analizo in poročanje. Sistem se zelo dobro povezuje s *Cloud-based* aplikacijami (razpršena hramba podatkov).

2.3.2.6 Microsoft in Omada

Microsoft in Omada vsak posebej spadata v kvadrant izzivalcev. V Sloveniji pa je pri ponudbi Microsoftovega *Forefront Identity Management* sistema (oziroma njegove stare različice, ki se imenuje angl. *Identity Lifecycle Management*, v nadaljevanju ILM) najbolj opazno dejstvo, da večina velikih podjetij po svetu uporablja aktivni imenik, ki sem ga podrobneje predstavil že v uvodnih poglavjih, zato se mnogo kupcev, ki išče alternativo vodilnim, najprej obrne na Microsoft, ki je v mnogih primerih dobavitelj vsaj namiznih operacijskih sistemov kot tudi strežniške platforme in niza storitev, kot so datotečne storitve itd. Krka je usmerjena predvsem v Microsoftove rešitve, ki so na slovenskem trgu tudi zelo dobro podprte – kar je tudi eden izmed razlogov, da v predstavitev vodilnih vključujem kombinirano rešitev podjetij Microsoft in Omada (kar je tudi rešitev, ki smo jo izbrali v Krki).

Bistvena prednost Microsoftove rešitve je v zelo nizkih cenah licenc, ki so od 50 % do 65 % nižje kot pri vodilnih ponudnikih ter tesna povezanost z aktivnim imenikom in še nekaterimi drugimi sistemi (na primer Microsoft Exchange). Prva verzija predvsem zaostaja s stališča uporabniške izkušnje, ki je vse preveč bazirala na skriptnem načinu nastavljanja konfiguracij, zato je bilo delo s tem sistemom za uporabnike sila neprijetno. Čeprav je Microsoft posamezne komponente sistema ILM združil pod skupno ime šele leta 2007, pa so že v letu 2003 imeli izdelan dober sistem za dodeljevanje pravic (angl. *Provisioning System*), po drugi strani pa se je podjetje Omada usmerilo v drug aspekt IdM sistema – to je uporabniška izkušnja, medtem ko lastni Provisioning System v večini bazira na Microsoftovem *FIM Synchronization Service*. Osnova Microsoftovega pristopa je torej *meta-imenik* z dobro izdelanim sistemom dodeljevanja pravic in velikim naborom agentov, medtem kot Omada doda pregleden in enostaven uporabniški vmesnik ter tudi nekaj svojih agentov za dodeljevanje pravic.

Prav tako kot ostali kombinirana rešitev Microsoft in Omada podpira: upravljanje uporabniških dostopov, upravljanje gesel, upravljanje življenjskih ciklov vlog, upravljanje dostopov do digitalnih virov, upravljanje zveznih identitet, sledenje, analizo in poročanje.

2.3.3 Izbor in ostali ponudniki

Podjetje ima torej kaj nekaj možnosti izbire med dobavitelji, tako vodilnimi kot ostalimi. Seveda to ne pomeni, da se morajo vsi kupci odločati predvsem med vodilnimi ponudniki, saj kot vidimo imajo le-ti res dobro izdelane celovite sisteme z mnogimi partnerji po celem svetu, vendar je s tega stališča pričakovati tudi najvišje cene. Cena predstavlja za marsikatero podjetje, ki se šele odloča oziroma razmišlja o vpeljavi IdM sistema, ki bo dolgoročno reševal težave z obvladovanjem ažurnega stanja identitet v podjetju, precej velik faktor pri izbiri. Torej kljub temu, da sem predstavil samo vodilnih pet ter kombinacijo Microsofta in Omade kot šestega ponudnika – ki je bil na koncu tudi izbran, si morajo v vsakem podjetju približje ogledati tudi ponudnike, ki niso v kvadrantu vodilnih, saj morda so manj izpopolnjene rešitve včasih celo boljše in lažje za vpeljavo ter predvsem cenovno bolj ugodne.

Če se vrnemo h Gartnerjevemu magičnemu kvadrantu, lahko ugotovimo, da so vsi ponudniki, ki so bili predstavljeni, že tudi veljavni ponudniki storitev upravljanja identitet v svetu, sicer ne bi bili vključeni v analizo. Kar v kratkem pomeni, da imajo vpeljan vsaj en lastni sistem in imajo stranke, ki ga uporabljajo. Torej je ključnega pomena pri izbiri prisotnost partnerja. V Sloveniji smo zaradi svoje majhnosti včasih prisiljeni iskati rešitve s tujimi partnerji, vendar je danes v Sloveniji na področju upravljanja identitet pristnih kar nekaj slovenskih podjetij, ki že imajo realizirane IdM projekte – torej imajo reference, po katerih je tudi odločitev bistveno lažja.

Osebnostno menim, da je Gartnerjev magični kvadrant dobro izhodišče pri iskanju IdM ponudnikov, potrebno pa ga je nagrajati še z lokalno ponudbo. Sami smo v Krki iskali tri konkurenčne ponudbe s področja IdM rešitev in samo IBM Tivoli ponudba je bila iz okvira vodilnih ponudnikov, ostale dve pa iz ponudbe izzivalcev (Microsoft skupaj s podjetjem Omada in SAP) oziroma SAP celo iz skupine igralcev, ki imajo rešitev izdelano za določene segmente (angl. *niche players*), ki pa navadno ne pokrijejo vsega segmenta poslovanja.

Zavedati se moramo, da so Gartnerjeve analize narejene navadno zelo široko in se občasno ne ujemajo s potrebami posameznikov, ki imajo posebne zahteve v svoji branži. Čeprav moramo priznati, da je skupina Gartner sestavljena iz skupine strokovnjakov, ki se dnevno ukvarjajo z raziskovanjem tržišča in so zagotovo njihove analize vredne ogleda in upoštevanja pred začetkom razmišljanja o vpeljavi sistema upravljanja identitet. Sama

odločitev pa je na koncu prepuščena nam, tudi v okviru naših finančnih zmožnosti in še bolj pomembno, samega dejanskega obsega poslovanja, ki ga želimo pokriti s sistemom upravljanja identitet.

2.3.3.1 Pristop k analizi ponudb

Podatki iz ponudb so strogo zaupni podatki med naročnikom in dobaviteljem, zato dejanskih podatkov analize ne morem predstaviti v nalogi, lahko pa predstavim princip izbire dobavitelja in sistem uteži pri izbiri. Za potrebe naloge sem se odločil, da pripravim analizo med najbolj zanimivimi ponudniki na slovenskem trgu. V prvi vrsti je zanimiv Oracle kot vodilni (L1 – *Leader 1*), potem prvi izzivalec na slovenskem tržišču, ki je zagotovo Microsoft, saj ima zelo močne partnerske naveze in sistemska okolja (C1 – *Challenger 1*) in prvi nišni igravec (NP1 – *Niche Player 1*), ki je v tem primeru SAP, ki ima tudi zelo dobre partnerske naveze z večjimi podjetji zaradi svojega ERP sistema. Da bi bila simulacija izbire med dobavitelji kar čim bolj realna, bom kot grobo okolje podjetja vzel dejansko **okolje** in stanje podjetja Krka, d. d., predpostavil pa bom, da ima podjetje **najtesnejšo partnersko zvezo** z izzivalcem (C1), ki tudi najbolje pozna okolje in **sistem dokumentacije** po izbranih smernicah (ITIL in GMP predstavljeno v poglavju 2.3) ter samo **vizijo** pri uvedbi sistema upravljanja identitet. Zelo pomemben pogled predstavlja tudi **cena**, ki sicer ni najpomembnejši dejavnik, vendar smo pogosto že imeli primer, kjer cena določenega ponudnika toliko odstopa od ostalih ponudb, da se celo pojavi dvom o verodostojnosti take ponudbe in seveda moramo nastaviti uteži temu primerno v analizi.

Lastnosti dobaviteljev. Vodilni ponudnik rešitve Oracle (L1) ima prestižno celotno orodje za povezovanje več sistemov, ki v celoti pokriva potrebe naročnika. Vodilni ima sicer dobre reference, vendar manj referenc v Sloveniji in manj referenc pri pokrivanju farmacevtske industrije ter slabše poznavanje standardov na področju farmacevtske industrije. Partnerski odnos z naročnikom obstaja, vendar v manjši meri (občasni nakupi opreme, posameznih rešitev podjetja Oracle – kot so podatkovne baze). Ponujena rešitev se dobro vključi v obstoječe okolje, čeprav zahteva nekaj nestandardnih sprememb v obstoječem okolju podjetja. Uporabniški vmesnik je enoten in funkcionalen, sinhronizacijska storitev omogoča sinhronizacijo vseh sistemov, predstavljenih v uporabniških zahtevah. Cena je zelo visoka.

Izzivalec Microsoft (C1), kot sem omenil prej, ima v prvi vrsti zelo dober partnerski odnos z naročnikom in ponuja enega izmed boljših sinhronizacijskih servisov. V podjetju se v veliki meri uporabljajo Microsoft tehnologije, zato je stopnja integracije Microsoft sistema pričakovano visoka, po drugi strani pa Microsoft ne ponuja neposrednega vmesnika za upravljanje identitet, pač pa uporablja dodatno tehnologijo *Microsoft SharePoint Portal Serverja* kot vmesnika za upravljanje FIM modula. Samo upravljanje identitet pa naj bi

potekalo v povezanih sistemih – na primer upravljanje uporabnikov skozi aktivni imenik. Cena je visoka, a vseeno nižja kot vodilni ponudnik.

SAP NetWeaver IdM, kot predstavnik niše (NP1), ponuja manjši nabor funkcionalnosti kot L1 in C1, vendar kljub temu zagotavlja osnovno funkcionalnost pri upravljanju identitet po uporabniških zahtevah, dolgoročno pa podpira manjši nabor sistemov kot ostala dva. SAP je sicer dolgoletni partner podjetja Krka, vendar izključno pri dobavi ERP sistema SAP R/3, ki pa ne pokriva avtomatizirane proizvodnje v Krki. SAP ima sicer dovršene izdelke, je pa s stališča podjetja precej togo podjetje, ki se na spremembe odziva počasneje kot ostali, razlog je predvsem v enotnosti produkta SAP R/3 pri mnogih strankah. Cena je visoka.

Opis dobaviteljev opreme. Na osnovi razpisne dokumentacije in pripravljenih uporabniških zahtev, ki smo jih podali ponudnikom, smo prejeli ponudbe naslednjih podjetij:

- L1 predstavlja ponudbo dobavitelja opreme Oracle Identity Manager.
- C1 predstavlja ponudbo dobavitelja opreme Microsoft FIM.
- NP1 predstavlja ponudbo dobavitelja opreme SAP NetWeaver.

Ponudniki so oddali ponudbe pravočasno ter jih tudi predstavili na uvodni predstavitvi (za potrebe analize predstavitve sem uporabil informacije na spletnih strani posameznega ponudnika).

L1 torej predstavi celostni produkt Oracle Identity Manager, predstavi tudi novitete pridobljene z nakupom podjetja Sun in novosti pri integraciji Oracleovih produktov s Sunovimi. Oracle ponuja sinhronizacijski servis, upravljanje uporabnikov, upravljanje življenjskega cikla ter upravljanje na podlagi vlog.

C1 predstavi predvsem sinhronizacijske prednosti produkta Forefront Identity Manager ter zagovarja upravljanje uporabnikov skozi klasične vmesnike v Windows okolju. Sinhronizacija temelji na uporabi meta-imenika, ki prečrpava podatke med raznimi sistemi. Posebej prilagojenih spletnih vmesnikov sistem ne ponuja, ponujajo pa opcijsko dograditev funkcionalnosti z vmesniki partnerskega podjetja Omada, ki pa ni predmet te analize, čeprav smo v Krki dejansko izbrali kombinirano ponudbo podjetij Microsoft in Omada. Microsoft FIM ponuja sinhronizacijski servis in upravljanje uporabnikov, težje izvedljiva pa sta upravljanje življenjskega cikla na podlagi vlog.

NP1 predstavi svojo rešitev SAP Netweaver Identity Management, ki ponuja dodeljevanje uporabniških pravic v heterogenem okolju. Za dodeljevanje uporabniških pravic v SAP

okolju ima SAP drugo orodje – SAP GRC. Slabost SAP ponudbe je v razdrobljenem upravljanju in pomanjkanju agentov za množico podsistemov uporabljenih v Krki. SAP nima enotnega vmesnika ter ima okrnjen sinhronizacijski servis za potrebe v Krki, a dovolj funkcionalnosti za izvedbo osnovnih principov upravljanja identitet.

Kriteriji primerjave. Produkte smo primerjali po naslednjih kriterijih:

- Cena: primerjava cen je narejena za 7000 uporabnikov.
- Skladnost s Krkinimi standardi: primerjamo integriranost predlagane infrastrukture s Krkinimi obstoječimi sistemi; izkušnje Službe za ITT s predlagano infrastrukturo.
- Ustreza Krkini viziji, strategiji: vsi trije produkti v popolnosti ustrezajo Krkini viziji na področju upravljanja z uporabniki.
- Cena vzdrževanja.
- Referenca: ocenjevali smo število in kvaliteto referenc partnerjev s poudarkom na Sloveniji in farmacevtski industriji. Reference v Sloveniji ima samo Microsoft. Microsoft s partnerjem Omada in SAP ima reference tudi pri večjih farmacevtskih podjetjih.
- Zaupanje v dobavitelja.
- Kvalitetni nivo predstavitve.
- Ustreznost glede na zahteve: ocenjevali smo odgovore dobaviteljev na uporabniške zahteve v pisni obliki in dodatna pojasnila ob predstavitvi (na spletnih straneh).
- Tehnična plat rešitve:
 - Oraclovo rešitev smo ocenili kot najbolj popolno in celovito.
 - Microsoftova po funkcionalnosti ne zaostaja, vendar za rešitev predlagajo dodatni produkt (ILM, in OID).
 - SAP pa ima za to področje dva produkta, kjer ne obstaja jasna razmejitev med njima niti konkretna vizija razvoja teh produktov v prihodnosti.
- Vpliv na obstoječe Krkino okolje: ocenjevali smo vpliv na obstoječe Krkine sisteme in aplikacije (ali so na obstoječih sistemih potrebne spremembe ali posegi).
- Upravljanje in kompleksnost sistema.

Za vsak kriterij smo uporabljali ocene od 1 do 5. Pomen ocen pa je naslednji:

- 1 – nesprejemljivo,
- 2 – slabo,
- 3 – dobro,
- 4 – zelo dobro,
- 5 – odlično.

Sestavili smo tabelo 3, v katero smo za vsak kriterij vsakemu ponudniku dodelili oceno.

Tabela 3: Tabela kriterijev, uteži in ocen ponudnikov

Kriterij	Uteži	L1			C1		NP3	
Cena	6	4	24	5	30	4	24	
Skladnost z internimi standardi	7	4	28	5	35	4	28	
Ustreznost glede na vizijo, strategijo	9	5	45	5	45	5	45	
Cena vzdrževanja	9	3	27	3	27	4	36	
Referenca	6	3	18	4	24	4	24	
Zaupanje v dobavitelja	7	4	28	5	35	5	35	
Kvalitetni nivo predstavitve	2	5	10	4	8	3	6	
Ustreznost glede na zahteve uporabnikov	10	5	50	5	50	4	40	
Tehnična plat rešitve	9	5	45	4	36	3	27	
Vpliv na obstoječe okolje	8	5	40	5	40	4	32	
Upravljanje in kompleksnost sistema	6	5	30	5	30	3	18	
Skupna ocena			345		360		315	

Podrobna ustreznost glede na zahteve uporabnikov (iz točke 3.2) prikazuje tabela 4:

Tabela 4: Tabela ustreznosti ponudnikov glede na uporabniške zahteve

	L1	C1	NP1
Baza podatkov o zaposlenih	5	5	5
Upravljanje z identitetami skozi celoten življenjski cikel	5	4	5
Sinhronizacija aktivnega imenika in kadrovskega informacijskega sistema	5	5	4
Samoadministracija uporabniških parametrov	5	5	5
Aplikacije, baze podatkov	5	4	4
Upravljanja s certifikati	5	5	5
Delovni procesi (workflow)	5	5	5
Single Sign-on	5	5	5
Poročila in statistike	5	5	3
Povprečna ocena	5,00	4,78	4,56

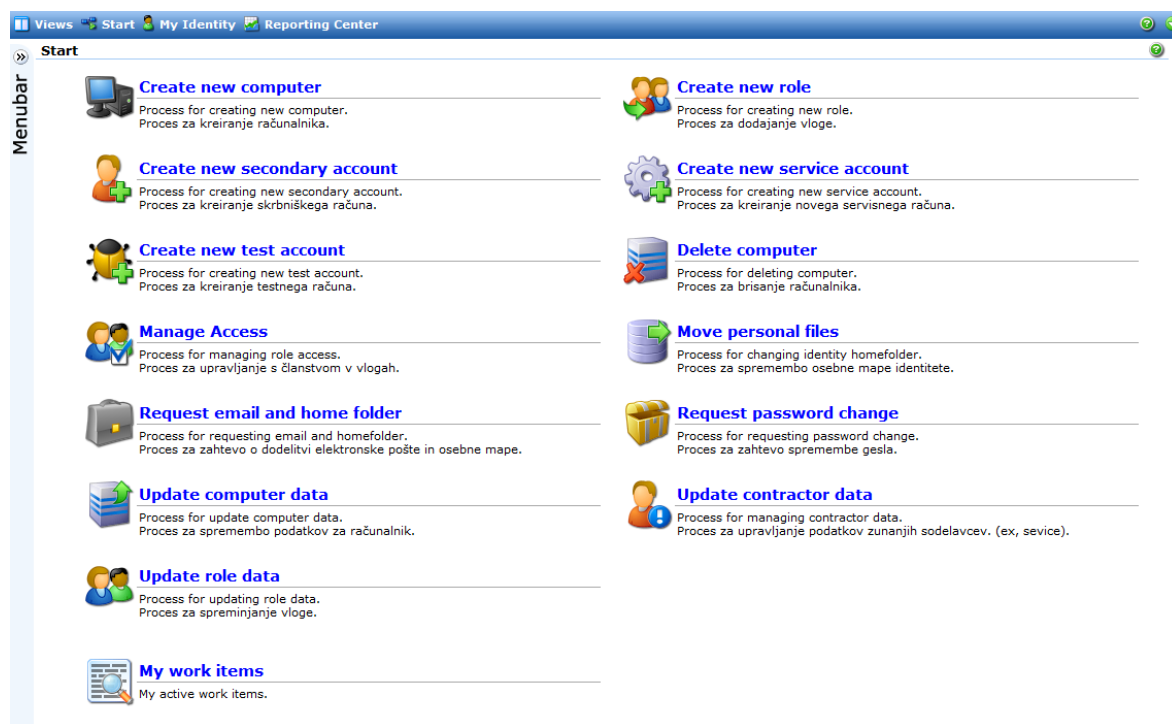
Vsi trije predstavljeni produkti so kvalitetni in izpolnjujejo uporabniške zahteve. Glede na sistem uteži in podrobno predstavljenih odgovorov glede na uporabniške zahteve je ponudnik Oracle, kljub nekaterim okoljskim razlikam, še vedno najbolj primeren ponudnik za kompleksno okolje podjetja Krka. Glavna slabost Oracleove ponudbe je v tem, da njihova rešitev prinaša preveč novosti v Krkino okolje. SAP (NP1) je v tej simulaciji najslabši ponudnik, saj način upravljanja, priprave poročil in statistik močno odstopajo od konkurenčne ponudbe ter mu tako precej znižujejo skupno oceno. SAP bi bil primeren v manjšem obsegu, kjer bi večino poslovanja obvladovali že skozi SAP R/3 ERP sistem – v Krki pa to pokrije samo manjši poslovni segment v podjetju. Slabost SAP je tudi v zelo kompleksni rešitvi in sama vizija razvoja je nejasna.

Prednost ponudnika Microsoft (C1) pa je vpetost v obstoječe Krkine sisteme, rešitev je enostavna, jasna in uporabniško prijazna. Edini pomislek pri njihovi rešitvi so uporabniški

vmesniki, ki niso zasnovani kot spletni vmesniki, pač pa skozi obstoječe metode upravljanja identitet – na primer vmesnik za aktivni imenik itd. Microsoft se zaveda pomanjkljivosti v uporabniških vmesnikih zato kot partnersko podjetje navaja Omada, ki pa zapolnjuje vrzel uporabniške izkušnje in delovnih tokov pri upravljanju identitet.

V Krki smo na podoben način izbirali med nekaterimi ponudniki IdM rešitev v Sloveniji ter se na koncu odločili za rešitev podjetij Omada in Microsoft **skupaj** (v tabeli vidimo, da Oracle ne vodi bistveno, če Microsoftovi ponudbi dodamo ponudbo podjetja Omada). Kot sem omenil, se Microsoftov FIM izkaže kot odličen sinhronizacijski servis, medtem ko Omada ponuja spletne vmesnike za upravljanje identitet in življenjskih ciklov vlog. Spletni vmesnik Omade, je prikazan na sliki 11 in predstavlja končni izdelek za uporabnika.

Slika 11: Vmesnik Omada



3. VPELJAVA SISTEMA UPRAVLJANJA IDENTITET V PODJETJE

3.1 Predstavitev podjetja Krka, d. d.

Krka, d. d., Novo mesto (v nadaljevanju Krka) je mednarodno farmacevtsko podjetje, prisotno na trgih Zahodne, Vzhodne in Srednje Evrope, Amerike in Ruske federacije. Približno petino proizvodnje prodamo na domačem trgu, ostalo pa izvozimo. Še vedno je najmočnejši trg Ruske federacije, vendar je Krka v letu 2007 uspešno okrepila tudi trg Zahodne Evrope. Konec leta 2010 je bilo zaposlenih približno 8800 delavcev (konec leta 2003 je bilo v Krki zaposlenih »samo« nekaj več kot 3.000 delavcev). Največji porast je bil med leti 2003 in 2008, zadnje 2 leti pa se je št. zaposlenih umirilo, kar je tudi razlog krize zadnjih let.

Uspešna rast in hiter razvoj Krke od njene ustanovitve leta 1954 pa do danes sta v veliki meri zasluga strokovno usposobljenih in motiviranih ljudi, ki so sledili vsem zahtevam stroke. Nenehno vlagamo v znanje, usposabljanje zaposlenih ter v posodabljanje tehnološke opreme. Vse svoje zmogljivosti usmerjamo v razvoj lastnih z blagovnimi znamkami zaščitene zdravil, ki so učinkovita, kakovostna, varna in cenovno sprejemljiva.

V farmacevtsko-kemijski dejavnosti je zajetega več kot 90 % Krkinega poslovanja. Ta dejavnost vključuje proizvodnjo in prodajo zdravil za humano uporabo, izdelkov za samozdravljenje ter veterinarskih izdelkov (proizvodnja kozmetičnih izdelkov je bila v letu 2006 opuščena).

Krkina dolgoročna strategija temelji na razvoju in prodaji generičnih farmacevtskih izdelkov pod lastnimi blagovnimi znamkami. Z njimi, v manjši meri pa tudi z izdelki licenčnih partnerjev, bomo tudi v prihodnje uporabnikom zagotavljali kakovostna, varna in učinkovita zdravila. Zato smo tehnološko zahtevno in okolju prijazno proizvodnjo uskladili z najvišjimi mednarodnimi standardi.

V Krki se zavedamo, da bomo v vedno hujši tekmi le s premišljenimi poslovnimi odločitvami in primerno organizacijo lahko uresničevali načrtano strategijo razvoja družbe in ostali med vodilnimi farmacevtskimi podjetji na tržiščih, kjer smo prisotni. Tudi zato smo se odločili za sodobno vodenje poslovnih procesov in temu sorodno modernejšo organizacijo družbe. Tako bomo še naprej ustvarjali priložnosti za izboljševanje vseh Krkinih procesov in rezultatov. Tak pristop pa nam bo hkrati omogočal doseganje vrhunske kakovosti izdelkov, večjo ekonomičnost, hitro odzivnost in sožitje z okoljem (nenazadnje tudi konkurenčno prednost).

Poslanstvo Krke je »Živeti zdravo življenje« in naša vizija je utrditi položaj enega vodilnih

farmacevtskih podjetij na obstoječih trgih. To bomo še naprej dosegali z lastnim razvojem, mednarodnimi povezavami, fleksibilnostjo in učinkovitostjo. S tem bomo uresničevali svojo vizijo uglednega in prodornega, visoko inovativnega mednarodnega generičnega farmacevtskega podjetja.

3.1.1 Sektor za informacijske tehnologije in telekomunikacije

Sam sem že 10 let zaposlen v sektorju za informacijske tehnologije in telekomunikacije (v nadaljevanju SITT), katerega naloge so:

- ugotavljanje potreb po razvoju novih in nadomeščanju obstoječih obdelav,
- načrtovanje in uvajanje rešitev,
- vzpostavljanje računalniške infrastrukture,
- zagotavljanje delovanja,
- vzpostavljanje in uveljavljanje standardov,
- zagotavljanje kvalitete računalniških rešitev,
- načrtovanje izobraževanja in usposabljanja.

Projektno vodenje je ključna metodologija vpeljave novih sistemov, kjer sistem vpeljave novih rešitev zahteva pripravo in izvedbo ključnih korakov vsakega projekta:

- uporabniške zahteve,
- funkcionalna specifikacija,
- dizajn specifikacija (načrt rešitve),
- izdelava rešitve/parametrizacija,
- testiranje rešitve,
- usposabljanje uporabnikov za uporabo obdelav,
- uvedba rešitve,
- vzdrževanje obdelav (kontrola sprememb).

Vsi sektorji in službe v Krki so podvrženi strogim regulativam in standardom, ki predvidevajo uporabo naslednjih varnostnih mehanizmov (interna standardizacija):

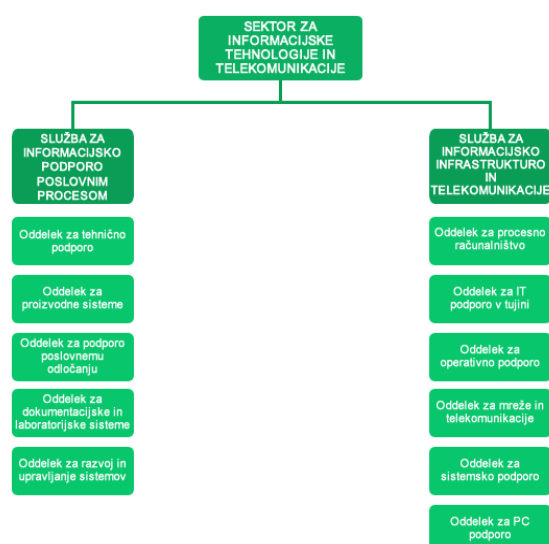
- veljajo predpisani Krkini standardi za strojno in programsko opremo,
- standardni poslovni sistem v podjetjih je Navision, povezan v Krkin direktorski sistem,
- uporaba varnih internetnih povezav (VPN) za oddaljena omrežja,
- centraliziran aktivni imenik (prijave v domeno),

- centralizirano izvajanje občutljivih aplikacij (spletni vmesniki, Citrix),
- oddaljena pomoč in upravljanje,
- centraliziran sporočilni sistem.

3.1.2 Službi v SITT

Sektor sestavljata službi **informatijske infrastrukture** in **podpora poslovnim procesom**. Službi si delita delo na področju informatike, in sicer na infrastrukturna dela, ki predstavljajo vse procese, ki služijo kot osnova za delo ostalim procesom (na primer mreža, aktivni imenik itd.), služba za poslovne procese pa skrbi za implementacijo poslovnih aplikacij glede na uporabniške zahteve in obstoječo infrastrukturo. Službi sodelujeta pri oblikovanju strategije za prihodnost tako poslovnih aplikacij kot infrastrukture. Slika 12 prikazuje strukturo sektorja SITT.

Slika 12: Služba informatike v Krki



Službe sestavljajo oddelki, kjer sta s stališča te naloge zanimiva predvsem dva oddelka, ki bistveno pridobita z vpeljavo sistema upravljanja identitet: oddelk za sistemsko podoro (angl. *System Support*) in oddelk za pomoč uporabnikom (angl. *Help desk* ali *Service desk*).

Oddelk za sistemsko podoro se ukvarja s temeljnimi infrastrukturnimi storitvami, kot so mreža, operacijski sistemi, diskovna polja ipd. Inženirji v oddelku sistemske podpore dnevno kreirajo objekte aktivnega imenika, postavljajo nove infrastrukturne storitve itd.

Oddelk za pomoč uporabnikom je vstopna točka vsem Krkinim zaposlenim, ki potrebujejo pomoč pri delu z osebnim računalnikom ali v primeru drugih težav, povezanih bodisi z računalniškim omrežjem ali drugimi podpornimi sistemi. Njena moč učinkovitega in hitrega odziva na uporabniške zahteve lahko bistveno izboljša ugled službe IT in hkrati omogoči tehničnemu osebju službe več časa za reševanje kompleksnejših problemov in razvoju novih storitev. Cilj službe je nudenje pomoči in podpore za vse IT storitve (e-pošta, mrežno tiskanje itd.) uporabnikom ter v prvi vrsti kreiranje teh objektov oziroma sprožitve procesa kreiranja objektov.

Bistvo službe iz pogleda tehničnih oddelkov pa je razbremenitev v smislu reševanja znanih težav, ki se pojavljajo na nižjem nivoju (v večini primerov obstajajo postopki, kako se neke znane težave rešujejo in zaposleni v službi za pomoč uporabnikov lahko s pomočjo teh postopkov sami pomagajo uporabniku v težavah). V ta okvir se šteje tudi kreiranje novih uporabniških računov, elektronskih poštnih naslovov, varnostnih skupin itd. Eden izmed ciljev uvajanja sistema upravljanja identitet je prav v skrajšanju časa, ki je potreben za izvedbo takšnih zahtevkov.

3.2 Uporabniške zahteve za vpeljavo sistema upravljanja identitet

Dobro pripravljene uporabniške zahteve lahko vsebujejo vse potrebno za izdelavo funkcionalne specifikacije in specifikacije načrta (angl. *Design specification*), potrebne po specifikaciji GMP. V Krki je priprava uporabniških zahtev najbolj kompleksno opravilo, saj zahteva zelo natančno opredelitev, kaj želimo izvesti in kako doseči zastavljene cilje. Dokumenti dobaviteljev, ki sledijo izdelanim uporabniškim zahtevam, so po eni strani zelo tehnični dokumenti, kjer so opisane posamezne tehnične nastavitve, po drugi strani pa je to tudi vsebinski odgovor na uporabniške zahteve.

Poglavje predstavlja jedro naloge, saj je izdelava podrobnih uporabniških zahtev najbolj zahtevna naloga s strani naročnika (v tem primeru podjetja Krka) ter vsebuje pregled stanja, opis sistemov in procesov, definirane cilje in končno konfiguracijo sistema. Zaradi obsega projekta smo se lotili pristopa fazno, kjer smo v prvi fazi vpeljevali sistem upravljanja identitet za uporabnike, definirane v aktivnem imeniku, kadrovske bazi in sistemu elektronske pošte. Prva faza je v Krki v celoti zaključena, trenutno pa se pripravljamo na vpeljavo druge faze projekta, in sicer upravljanja vlog v sistemih.

Za potrebe magistrske naloge bom v nadaljevanju poglavja opisal korake, po katerih smo v podjetju izvajali vpeljavo sistema upravljanja identitet, torej upravljanje uporabnikov ter postopke vpeljave sinhronizacije aktivnega imenika in kadrovskega informacijskega sistema.

3.2.1 Predstavitev trenutnega stanja

Upravljanje z uporabniki je pereč problem sodobnih organizacij, kar občutimo tudi v Krki. Zaposlenih je več kot 8.000 oseb, od katerih ima večina tudi izdelana uporabniška imena za prijavo v Krkino omrežje osebnih računalnikov. Postopki izdelave novih računov, vzdrževanje podatkov o računih, spremembe ter še posebej povezane spremembe (torej tiste, ki se dotikajo ostalih sistemov) na ostalih sistemih in aplikacijah, čakajo realizacijo

vseh potrebnih skrbnikov celo več dni, kar ohromi delo posameznikov in vključuje možnost človeške napake, ki je pri velikem obsegu tipske dela tudi zelo pogosta.

V večjih informacijskih sistemih se srečujemo s krizo identitet predvsem iz naslednjih razlogov:

- uporabljamo veliko sistemov in aplikacij,
- vsak uporabnik ima več identitet v različnih sistemih in aplikacijah,
- identitete se spreminjajo (življenjski cikel identitete).

Posledično imamo zaradi tega naslednje težave:

- časovno zahtevno in drago vzdrževanje identitet,
- slaba preglednost in sledljivost izvedenih sprememb,
- slaba produktivnost zaradi neažurnih sprememb,
- omejena integracija sistemov in aplikacij,
- varnost iz naslova neažurno odstranjenih pravic in dostopov.

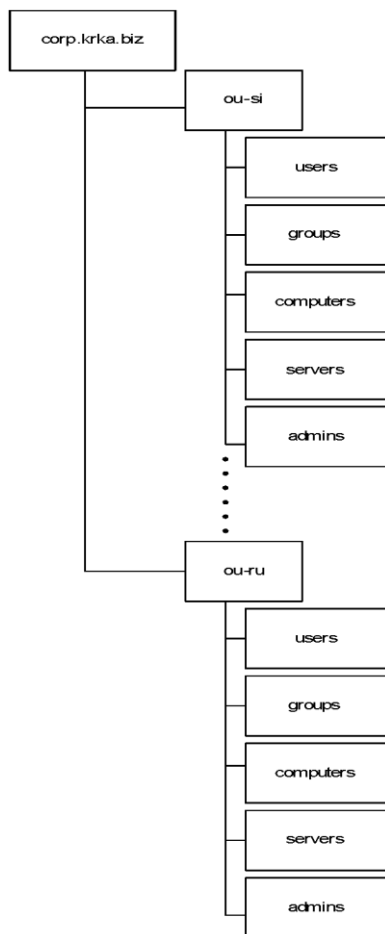
Zato moramo poskrbeti, da se nedvoumno določi identiteta uporabnika in poenostavi in pohitri postopke upravljanja z uporabniki. Cilji vpeljave sistema za upravljanje uporabnikov so:

- avtomatizacija oziroma poenostavitev postopkov za dodeljevanje pravic uporabnikom,
- zmanjšanje števila napak pri dodeljevanju pravic uporabnikom,
- zmanjšanje potrebnega časa za postopke obvladovanja identitet v procesu zaposlitve, prerazporeditve ali izstopa zaposlenega,
- omogočanje enotnega vpogleda v podatke o uporabniških identitetah,
- zmanjševanje tveganj zaradi zlorabe osebnih in zaupnih podatkov v podjetju,
- podpora aplikativnim rešitvam z velikim številom uporabnikov,
- izboljšanje integracije sistemov in aplikacij.

3.2.2 Opis trenutnega stanja aktivnega imenika

Notranji aktivni imenik. V podjetju imamo Microsoft Windows 2003 domeno. Večino upravljanja aktivnega imenika se izvaja na centralni lokaciji v Novem mestu, določene naloge pa izvajajo tudi operaterji na oddaljenih lokacijah (lokacije v Sloveniji in tujini).

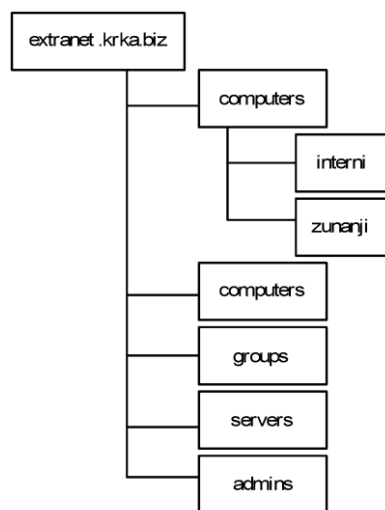
Slika 13: Notranji aktivni imenik



Kar nekaj nalog je delegiranih, določene pa še vedno izvajajo skrbniki. Aktivni imenik se napaja z določenimi podatki iz kadrovske baze. Za to trenutno uporabljamo dva avtomatska postopka (skripti). Prvi kreira uporabnike iz kadrovske baze v aktivni imenik, drugi pa sinhronizira izbrane podatke iz kadrovske baze v aktivni imenik (enosmerno).

Na sliki 13 je prikazana logična struktura notranjega aktivnega imenika. Po posameznih državah, kjer lokalni skrbniki nudijo podporo lokalnim uporabnikom, imamo definirano organizacijsko enoto ou-[okrajšano ime države]. Znotraj teh organizacijskih enot pa so še enote za različne objekte (uporabniki, skupine, računalniki, strežniki, skrbniški objekti). Poleg teh organizacijskih enot po državah imamo še organizacijsko enoto z imenom ou-skr-corp, znotraj katere so enote za vzdrževanje (*maintenance*), servisne (pod katerimi tečejo določene storitve) in avtomatske uporabniške račune (računalniški terminali v proizvodnji).

Slika 14: Zunanji aktivni imenik



Zunanji aktivni imenik

Tudi ta domena je Microsoft Windows 2003 domena, ki je namenjena predvsem za uporabo s strani naših partnerjev (ekstranet spletna delovna mesta). Ker so v njem objekti izključno zunanjih partnerjev, ta imenik ni sinhroniziran s kadrovske baze. Obe domeni sta med sabo povezani s tehnologijo Microsoft Active Directory Federation Services, ki omogoča enosmerno avtentikacijo uporabnikov storitev v zunanjem omrežju s Krkino domeno, zaradi česar tudi ne potrebujemo vzpostavitve zaupanja med domenama. Slika 14 prikazuje zunanji aktivni imenik.

3.2.3 Zahteve delovanja sistema

Glede na opisano okolje imenikov, enot v imeniku in težav, s katerimi se soočamo, želimo po uvedbi sistema doseči določene funkcionalnosti, način delovanja ter vključitev predpisanih varnostnih mehanizmov in zaščite.

3.2.3.1 Opis funkcionalnosti

Sistem upravljanja identitet mora omogočati upravljanje objektov obeh aktivnih imenikov (notranji in zunanji) znotraj enega vmesnika, ki naj bo izveden kot spletni vmesnik, neodvisen od računalniške platforme, na kateri se uporablja. To pomeni, da imamo povezavo na oba imenika. Rešitev naj omogoča delegacijo opravil znotraj aplikacije. Poleg skrbniške vloge mora sistem omogočati možnost kreiranja različnih vlog, za katere definiramo različna opravila (kreiranje objektov, ponastavitev gesel, omogočanje in onemogočanje objektov itd.). Poleg izbire opravil mora sistem omogočati tudi izbiro področja, kjer se lahko ta opravila izvajajo.

Primer vloge 1: Skupina SOS lahko kreira uporabnika, ponastavi geslo, omogoči ali onemogoči uporabniški objekt itd. Področje teh opravil je na nivoju celotne Krke.

Primer vloge 2: Skupina ITT Rusija lahko omogoči ali onemogoči uporabnika, ponastavi geslo. Področje teh opravil je na nivoju organizacijske enote ou-ru.

Rešitev naj teče pod določenim servisnim računom, v kontekstu katerega se izvajajo vsa opravila.

Baza podatkov o zaposlenih. Sistem mora vsebovati bazo podatkov z osnovnimi podatki o zaposlenih. Trenutno imamo podatke o zaposlenih urejene v dveh aplikacijah:

- SAP HR in
- KIS – lastna aplikacija (na bazi podatkov Microsoft SQL server).

Sistem mora omogočati povezavo z obema aplikacijama za sinhronizacijo podatkov.

Uvoz podatkov. Omogočen mora biti popoln uvoz podatkov za vse zaposlene ali samo spremembe.

Atributi v bazi zaposlenih. Sistem mora omogočati definicijo atributov za zaposlene, ki

jih želimo vzdrževati.

Avtoritativni izvor podatka. Sistem mora omogočati, da za vsak atribut določimo avtoritativni izvor podatka.

Obvezni podatki, pomanjkljive informacije. V sistemu mora biti možno določiti obvezne podatke o zaposlenemu in definirati akcije (angl. *workflow*) v primeru manjkajočega podatka.

Sinhronizacija podatkov. Sistem mora omogočati različne urnike sinhronizacije podatkov. Predvidevamo dva načina dela: ročni in periodični (dnevni, mesečni ipd.).

Poročila. Sistem mora vsebovati možnost izdelave poročil o podatkih zaposlenega in spremembah podatkov o zaposlenemu. Vključevati mora tudi podrobna poročila o spremembah pripadnosti v domenskih skupinah.

Izvoz podatkov. Sistem mora omogočati izvoz podatkov o zaposlenih vsaj v naslednjih dveh oblikah: tekstovna datoteka in Microsoft Excel.

Sinhronizacija aktivnega imenika in kadrovskega informacijskega sistema. Vzpostavitev sinhronizacije s kadrovske baze. Vse spremembe v kadrovske baze naj se osvežujejo v aktivnem imeniku (samo enosmerno iz KIS v AD). Seznam podatkov, ki se sinhronizirajo, je v dokumentu »Priloga 2: Specifikacija sinhronizacije KIS-AD« (glej Prilogo 2).

Sistem mora sam zaznati naslednje kadrovske dogodke in omogočati poročila o teh dogodkih:

- izstop iz podjetja,
- vstop zaposlenega v podjetje,
- prehod med različnimi statusi zaposlenega,
 - prehod iz agencije ali študentskega servisa v Krko,
 - prehod med podjetji,
- ponovna zaposlitev.

Sistem mora omogočiti povezavo do podatkov o zaposlenih na dveh različnih okoljih

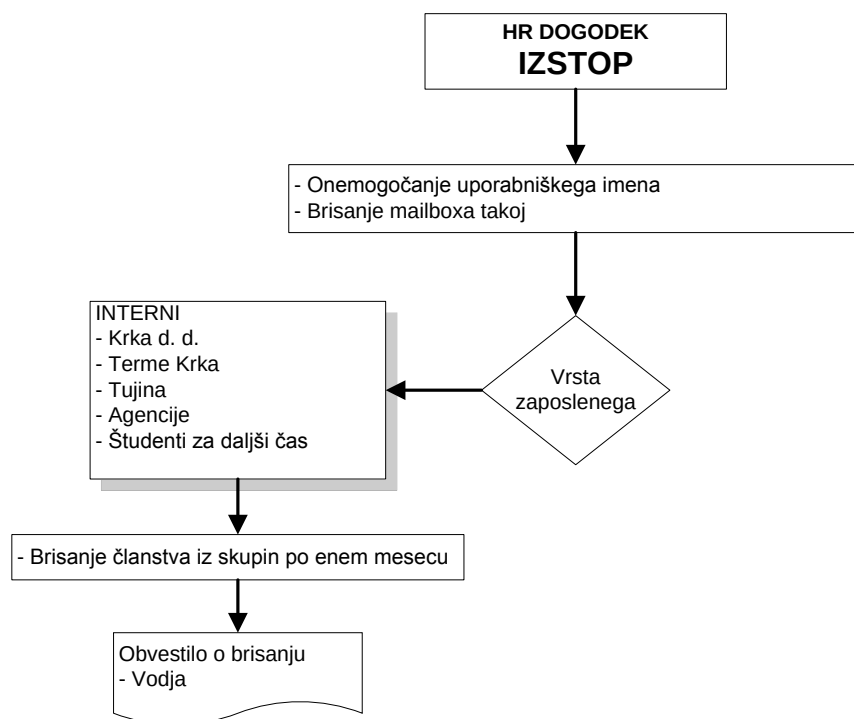
- SAP HR in
- lastna aplikacija (na bazi podatkov Microsoft SQL server).

Sistem mora omogočati delegacijo. To pomeni, da lahko uporabnik v IDM sistemu določi drugega uporabnika, ki bo v nekem časovnem obdobju prevzel njegove pravice in naloge in prejemal sporočila iz sistema. Uporabnik mora imeti možnost delegirati drugega uporabnika z naslednjimi podatki:

- Uporabniško ime,
- Datum pričetka,
- Datum zaključka.

Izstop. Proces ob **izstopu** zaposlenega je predstavljen na sliki 15. Ko v kadrovski bazi skrbnik ali operater izvede izstop zaposlenega, mora sistem ob prvi naslednji sinhronizaciji takoj onemogočiti račun uporabnika, in sicer za vse tipe uporabnikov (interni). Ko je uporabniški račun onemogočen, dostop do sistemov ni več mogoč. Onemogočen objekt se obdrži v vseh dodeljenih skupinah aktivnega imenika še 30 dni, po tem času pa se objekt odstrani tudi iz skupin aktivnega imenika in preko elektronske pošte obvesti vodjo.

Slika 15: Izstop



Vir: Interna dokumentacija Krka

Kreiranje uporabniških računov. Objekti naj se kreirajo čim bolj avtomatizirano s pomočjo podatkov iz kadrovske baze. Pri tem naj se prenesejo tudi določeni atributi. Ti so

definirani v dokumentu »Specifikacija sinhronizacije KIS-AD« (glej Prilogo 2). Pred kreiranjem mora sistem najprej ugotoviti, ali ta uporabnik že obstaja v aktivnem imeniku. Uporabniško ime določa aplikacija po ustreznem algoritmu.

Podrobnejši opis algoritma za kreiranje uporabniškega imena v sistemu upravljanja identitet naj predvideva naslednjo določitev uporabniškega imena: Če uporabniško ime, ki je določeno v točki X, že obstaja, algoritem tega ne uporabi in se premakne na točko X+1.

1. Uporabniško ime = priimek
2. Uporabniško ime = priimek + prva črka imena
3. Uporabniško ime = priimek + prva črka imena + druga črka imena + ...
- ...
4. Uporabniško ime = priimek + ime + zaporedna številka

Pri kreiranju uporabniških imen naj se upošteva pretvorba posebnih znakov, kot so: Č → C, Ć → C, Š → S, Ž → Z.

Logična struktura Krkega aktivnega imenika. Pri kreiranju uporabniških računov naj se upošteva logična struktura Krkega aktivnega imenika, kar pomeni, da se objekt na podlagi določenega vhodnega atributa kreira v ustrezni organizacijski enoti.

Kreiranje naslova elektronske pošte. Na osnovi podatka iz kadrovske baze se kreira elektronski naslov uporabnika. Poleg tega mora sistem upravljanja identitet omogočati ročno kreiranje elektronskega poštnega naslova (slika 16).

Slika 16: Dodatni naslov elektronske pošte

The screenshot shows a user profile form with the 'Organization' tab selected. The form contains the following fields and values:

Name	
First:	Matevž
Initials:	
Last:	Kristan
Display:	Kristan, Matevž
Alias: matevz.kristan	

Below the name fields, there are sections for Address, City, State, Zip code, Country/Region, Title, Company, Department, Office, Assistant, and Phone. The 'Add to Contacts' button is at the bottom left, and 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

Dodatni naslov elektronske pošte (angl. *alias*). Ob kreiranju osnovnega elektronskega

poštnega naslova mora sistem omogočati kreiranje dodatnega poštne predala, ki je formiran glede na algoritem ime.priimek oziroma ime.priimek in dodatna ustrezna zaporedna številka, da bo poštni predal unikatni znotraj organizacije. Ta poštni naslov je privzeti poštni naslov uporabnika.

Poštni strežnik. Sistem upravljanja identitet mora omogočati, da ob kreiranju elektronskega poštne naslova ponudi predlog za poštni strežnik in podatkovno skladišče glede na prvo črko priimka oziroma mora omogočati ročno izbiro poštne strežnika in podatkovnega skladišča (zaradi razdrobljenega sistema poštne strežnikov in skladišč).

Poštni strežnik za Terme Krka. Sistem mora omogočati uporabnikom iz organizacijske enote Terme Krka (posebna označba, ki je kljukica ali določena šifra podjetja), da se poleg standardnih poštne naslovov doda še naslov mailbox_alias@terme-krka.si, ki mora postati privzeti naslov.

Popravek podatkov poštne naslovov. Sistem mora omogočati spremembo podatkov zaradi sprememb priimkov (na primer ob poroki) na način ročnega urejanja podatkov, ki pa naj predlaga (ponudi) dodatni poštni naslov glede na algoritem ime.priimek1-priimek2 oziroma ime.priimek1-priimek in dodana ustrezna številka zaradi zagotavljanja enoličnosti poštne naslova znotraj organizacije. Sistem naj tudi omogoči spremembo podatkov prikaza imena (angl. *display name*) po algoritmu Priimek 1, Priimek 2, Ime. K obstoječim poštne naslovom se doda novi naslov ime.priimek1-priimek2@krka.biz in ga nastavi kot privzeti poštni naslov.

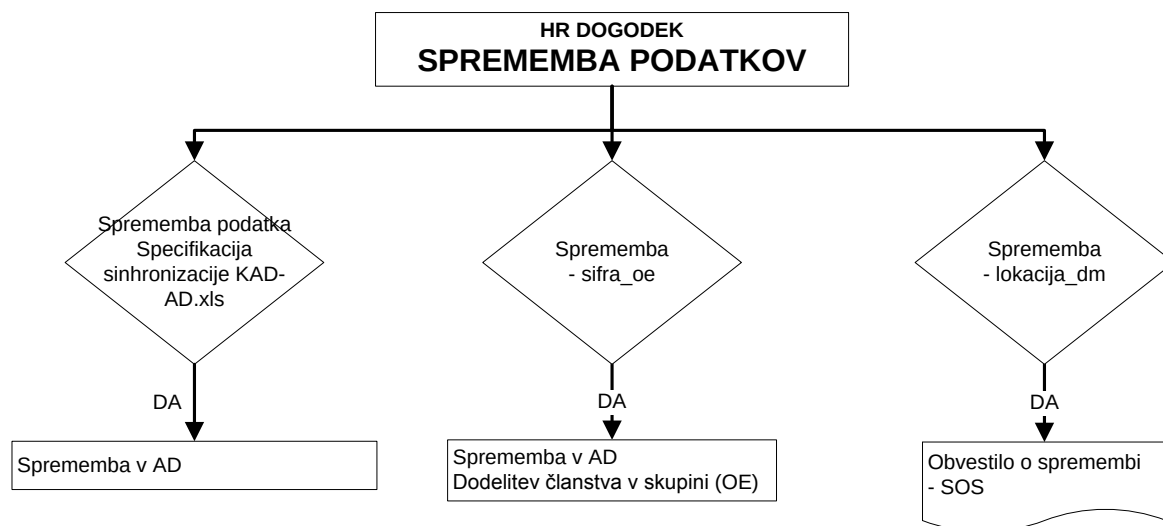
Distribucijska lista. Sistem mora omogočati, da ob kreiranju elektronskega naslova omogoča dodajanje uporabnika v ustrezno distribucijsko listo. Distribucijske liste se kreirajo po vlogah delovnih mest in niso obvezne, vendar je zaželena podpora upravljanja distribucijskih list v smislu menjave pripadnosti – enak način kot zamenjava pripadnosti domenskim skupinam.

Sprememba podatkov. Avtoritativni vir za kadrovske podatke je kadrovski informacijski sistem, kjer se tudi zavajajo potrebne spremembe podatkov zaposlenih. Slika 17 prikazuje proces avtomatske sinhronizacije podatkov med kadrovsko bazo (KIS) in aktivnim imenikom (AD).

Vse relacije med posameznimi atributi so opisane v dokumentu »Specifikacija sinhronizacije KIS-AD«. Ko se v sistem navede sprememba podatka, je možna izvedba treh akcij, kot prikazuje slika. Obvezno se zgodi sinhronizacija podatkov z aktivnim imenikom, kjer se nove spremembe prenesejo v aktivni imenik. V kolikor se spremeni tudi organizacijska enota zaposlenega, se mu spremeni tudi pripadnost v skupini organizacijske

enote. V kolikor se spremeni tudi lokacija delovnega mesta, pa je o tem potrebno obvestiti oddelek pomoči uporabnikom, ki poskrbi za prenos računalnika v novo pisarno ipd.

Slika 17: Sprememba podatkov

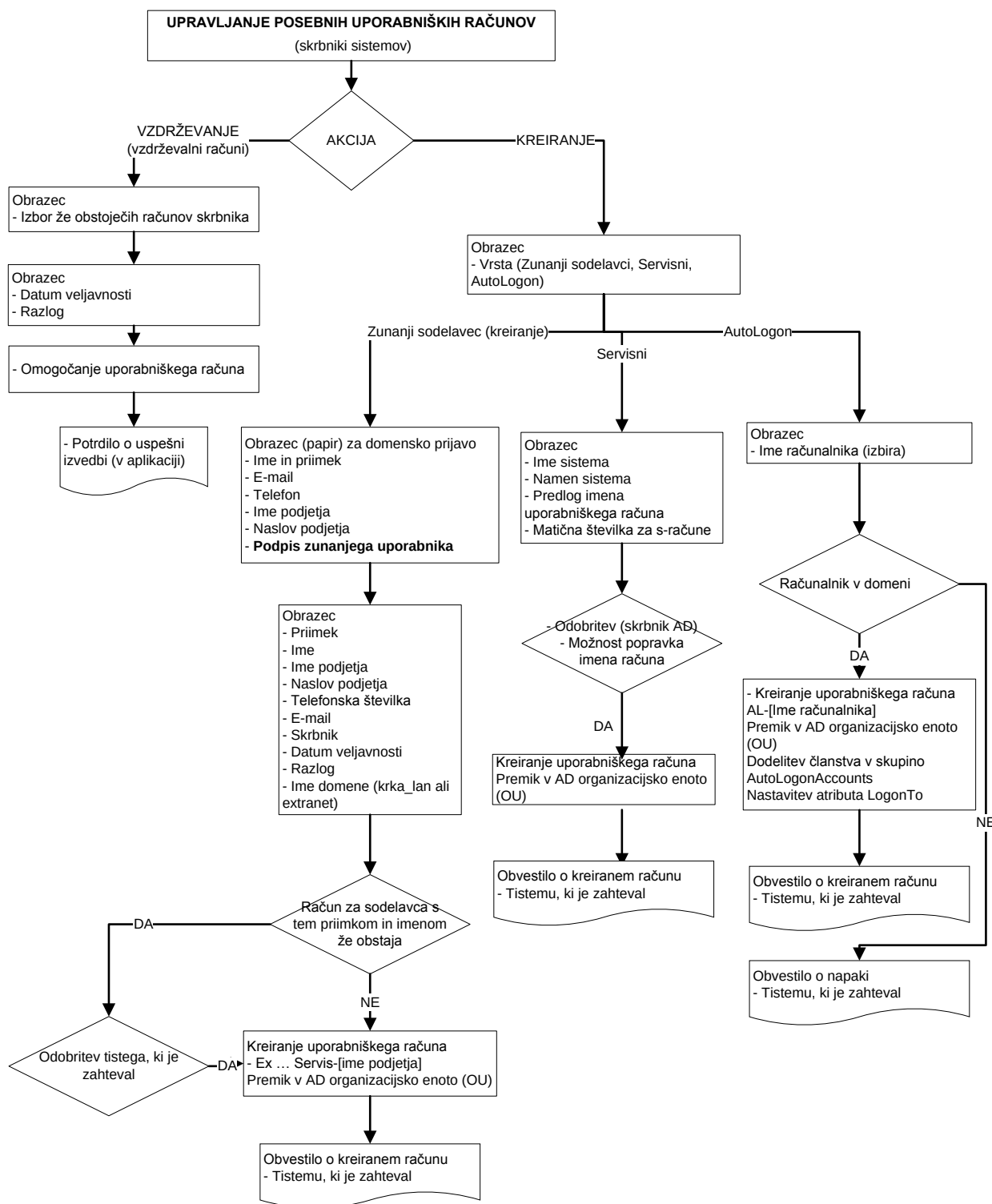


Vir: Interna dokumentacija Krka

Upravljanje posebnih uporabniških računov. Med posebne uporabniške račune zaenkrat štejemo le tri tipe računov. Zunanji sodelavci, ki potrebujejo dostop do Krkinega omrežja, dobijo uporabniški račun v domeni, s katero se lahko prijavijo v izbrane sisteme ter tako opravljajo svoje delo na sistemih. Kot vidimo na sliki 18 spodaj, je pri kreiranju teh računov potrebno izpolniti na obrazcu kar nekaj podatkov, ki so tipično podatki kadrovske baze za zaposlene. V tem primeru je avtoritativni vir podatkov aktivni imenik in ne kadrovska baza. Druga dva tipa posebnih računov pa sta t. i. »servisni« in »avto-logon« račun. Tip servisnih računov se uporablja v sistemih kot račun, ki poganja določeno storitev. V kolikor želimo doseči varno komunikacijo med dvema sistemoma, morajo storitve teh sistemov teči pod določenimi domenskimi računi, saj le tako sistema lahko opravita avtentikacijo med seboj in zagotovita varno komuniciranje. Avtologon računi pa se običajno uporabljajo v proizvodnji na računalnikih, ki jih uporablja več ljudi, brez lastne domenske prijave. V postopku spodaj vidimo, da sta možni akciji dve, in sicer vzdrževanje – torej odpiranje dostopa vzdrževalnim računom in kreiranje vseh treh tipov računov, kot sem opisal zgoraj.

Rešitev naj torej omogoča tudi kreiranje uporabniških računov na podlagi ročno vnesenih podatkov, torej kreiranje objektov, ki niso v kadrovski bazi (uprabniški računi za zunanje sodelavce, servisni računi, *avtologon* računi). Pri tem se ponudi izbira organizacijske enote, v kateri se potem kreira objekt.

Slika 18: Upravljanje posebnih računalniških računov

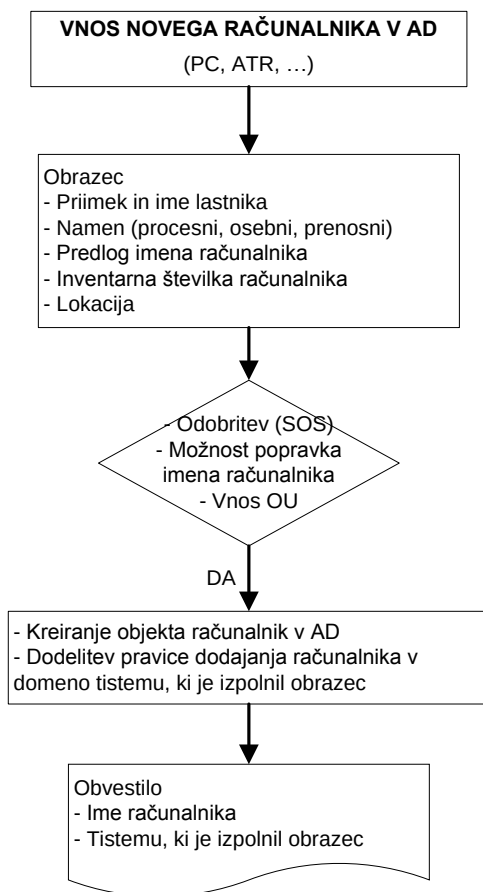


Vir: Interna dokumentacija Krka

Dodajanje računalnika v aktivni imenik. Sistem mora omogočati tudi dodajanje

računalnikov v aktivni imenik. Pred vsakim kreiranjem novega računalniškega objekta v AD-ju je potrebno najprej definirati lastniške podatke o novem računalniku (strežnik, osebni računalnik, ipd.). Te podatke potem potrdi oddelek za pomoč uporabnikom, ki ima opcijo popravka določenih podatkov zaradi skladnosti s pred pripravljeno imensko strategijo. Po odobritvi se kreira računalniški račun, dodeli ustrezne pravice in obvesti osebo, ki je zahtevala nov objekt (slika 19).

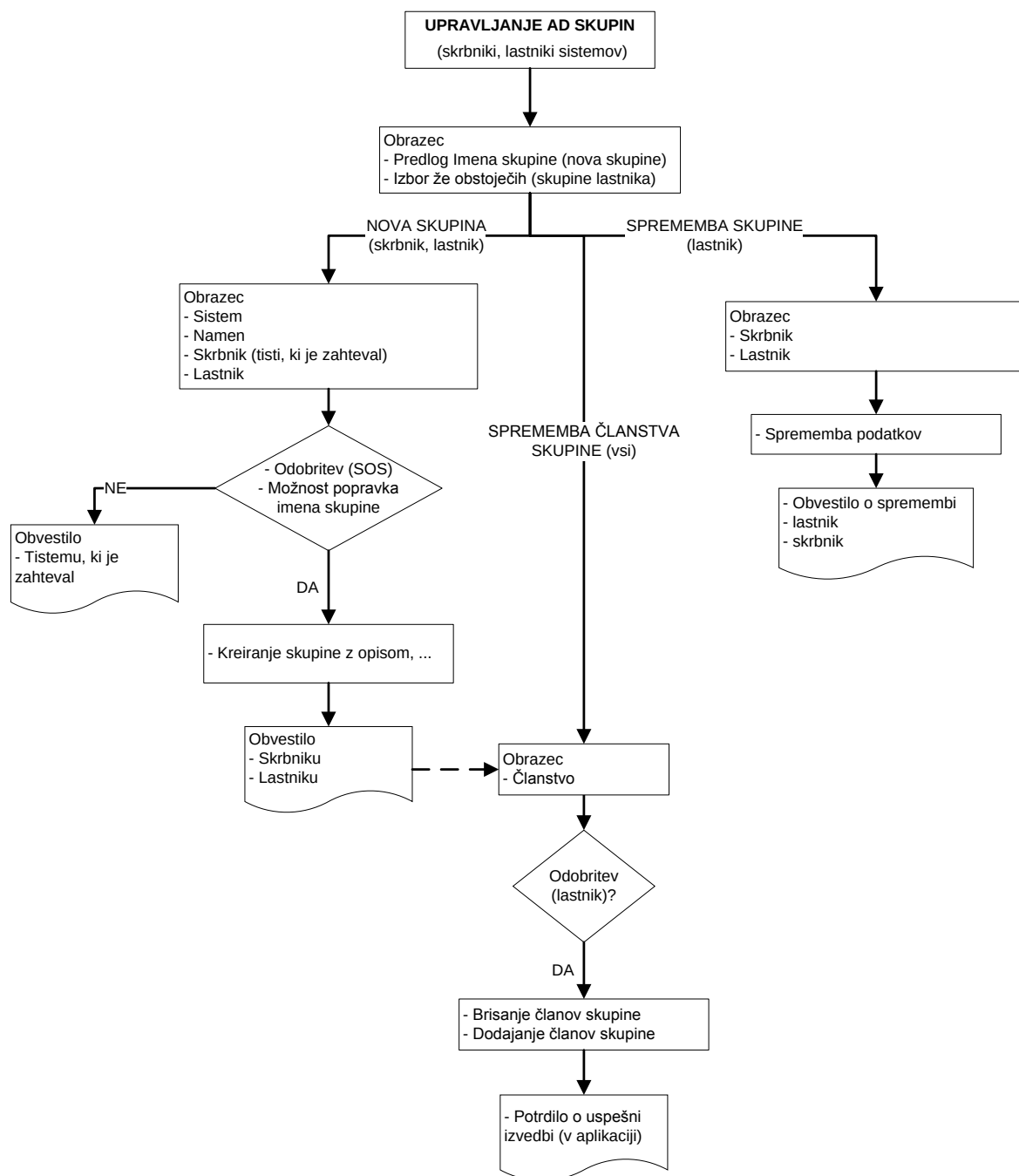
Slika 19: Dodajanje računalnika v aktivni imenik



Vir: Interna dokumentacija Krka

Upravljanje s skupinami. Za celostno upravljanje računov potrebujemo tudi upravljanje skupin, saj se po priporočilih Microsofta v večini primerov uporablja domenske skupine kot osnovne objekte za dodajanje pravic na sistemih. Sistem mora upravljati skupine tako od nastanka kot tudi do sprememb. Postopek upravljanja skupin torej delimo na 3 korake: kreiranje nove skupine, sledi odobritev, potem obvestilo lastniku in izvedba dodajanja uporabnikov v skupino. Sprememba članstva uporabnikov se izvede glede na zahtevo in odobritev, prav tako pa proces predvideva menjavo lastnika. Domenskih skupin v podjetju ne ukinjamo, zato postopek na sliki 20 tega ne predvideva.

Slika 20: Upravljanje s skupinami



Vir: Interna dokumentacija Krka

Smoadministracija uporabniških parametrov. Sistem naj omogoča tudi smoadministracijo za ponastavitev gesla uporabnikom preko spletnega vmesnika. Možno naj bo tudi ponastaviti geslo preko osebnega računalnika (Windows klasična menjava gesla). Predvidevamo tudi smoadministracijo povečevanja kapacitet domače mape (*home folder*) in dodatnega e-mail naslova – vendar se za oba zahteva odobritev vodje.

3.2.3.2 Načini delovanja

Sistem mora podpirati avtomatsko in ročno delovanje. Avtomatsko delovanje naj bo izvedeno z uporabo agentov, ki se povezujejo na sisteme. Ročno delovanje se delegira skrbnikom v obliki opravil, ki jih pošlje sistem preko pošte. Skrbnik mora po izvedenih zahtevkih potrditi opravljene naloge, kot bi to drug sistem javil avtomatsko ob uporabi agenta.

3.2.3.3 Napake in akcije ob možnih napakah

V Krki uporabljamo *Microsoft System Center Operations Manager 2007 (SCOM)* za nadzor nad delovanjem sistemov. Sistem obvešča o težavah in napakah preko elektronske pošte ali SMS storitve – kategorizacija je izvedena s posameznim skrbnikom sistema. Spremljanje napak naj bo integrirano v *SCOM-u* na tak način, da kritične napake v sistemu (na primer nedelovanje sinhronizacije ali uporabniškega vmesnika) javijo na dežurni telefon v obliki SMS sporočila, ostale težave pa uporabniki javljajo po elektronski pošti.

3.2.3.4 Varnost in zaščita zahtevana na sistemu

Sistem mora biti postavljen tako, da bo ustrezal vsem priporočilom varnostnih standardov ISO 17799, ISO 2700x in Krkini varnostni politiki. Za dostop do sistema se uporablja domenska prijava. Elektronski podpis ni v uporabi. Za vsa opravila se mora izvajati sledljivost (dnevnik aktivnosti):

- sledljivost za uporabniške račune (novi uporabniški računi, spremembe, kdo je izvedel, kdo zahteval, čas, možnost pregledov po atributih aktivnega imenika);
- sledljivost za skupine (opis grupe, nove grupe, spremembe, kdo je izvedel, kdo zahteval, čas, možnost pregledov po atributih iz aktivnega imenika, ...);
- vsi zapisi sledljivosti morajo biti nespremenljivi in neizbrisljivi (CFR 21 Part 11, FDA regulativa).

3.2.4 Podatki, zapisi ter podpisi v sistemu

Pomembna logična definicija potrebnih podpisov in zapisov ob avtomatskem izvajanju akcij mora ostati nespremenjena, lahko pa se postopek spremeni do te mere, da se določene odobritve konsolidirajo v manj korakih. Za vsak sistem določimo podatke, zapise in podpisnike ter jih analogno predstavimo tudi v novem sistemu. Zelo pomembno je tudi

spoštovanje t. i. (angl. *Predicate rules* – pravila, ki veljajo v državi, kjer proizvajamo, za katero proizvajamo, GMP pravila, FDA pravila - CFR21part11 in EUAnex11, predpisani interni Standardni operativni postopki).

3.2.4.1 Podatki

V sistemu se bodo nahajali naslednji podatki:

- Uporabniki:
 - uporabniško ime,
 - ime,
 - priimek,
 - matična številka,
 - veljavnost,
 - razlog,
 - ime podjetja,
 - naslov podjetja,
 - e-pošta,
 - telefon,
 - domena,
 - ime sistema,
 - namen sistema.
- Skupine:
 - ime skupine,
 - namen skupine,
 - skrbnik,
 - lastnik.
- Računalniki:
 - ime računalnika,
 - ime lastnika,
 - priimek lastnika,
 - namen,
 - inventarna številka.
- Sledljivost:
 - sledljivost za uporabniške račune,
 - sledljivost za skupine v AD.

3.2.4.2 Zapisi

Zapisov oziroma standardnih izpisov iz sistema ne potrebujemo. Sistem mora omogočati poizvedbe nad vsemi podatki. Specifike posameznih poizvedb bodo definirane v t. i. Funkcionalni specifikaciji v dogovoru z dobaviteljem. V osnovi se pripravi vsaj naslednje poizvedbe:

- seznam uporabnikov;
- podatki o uporabniku (splošno, članstvo v skupinah);
- komu je bil uporabniški račun omogočen;
- odobritve (kje zahteve čakajo);
- podatki o skupinah (zgodovina).

3.2.4.3 Podpisi

Elektronskega podpisa ne bomo uporabljali. V sistemu bodo naslednje odobritve (ki ne bodo izvedene z elektronskim podpisom):

- Odobritev vodje za kreiranje elektronskega poštnega naslova in domače mape;
- odobritev skrbnika aktivnega imenika za kreiranje skrbniškega računa in
- odobritev lastnikov procesov za članstvo v AD skupini.

3.2.4.4 Vmesniki

Uporabniški vmesnik z osnovnim opisom vlog. Uporabniški vmesnik naj bo izveden v okviru spletne aplikacije (uporabniškega vmesnika). Osnovne vloge uporabnikov v sistemu prikazuje tabela 5.

Vmesnik proti ostalim sistemom. Sistem bo v prvi fazi povezan na naslednje sisteme:

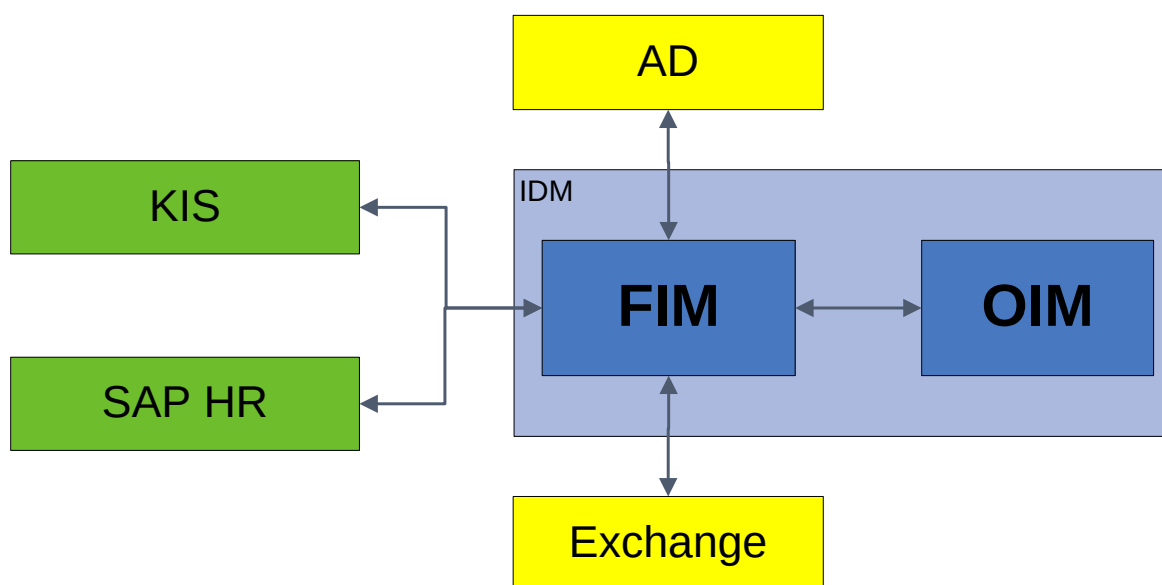
- Kadrovski informacijski sistem (KIS),
- SAP HR,
- aktivni imenik (AD),
- poštni strežnik (Microsoft Exchange).

Logično shemo povezanih sistemov predstavlja slika 21.

Tabela 5: Tabela vlog v sistemu

Skrbnik	Skrbnik aplikacije z vsemi pravicami
Lastniki procesov	Kreiranje nove skupine v AD Spremembe skupine v AD Spremembe članstva skupine v AD
Skrbniki procesov	Kreiranje nove skupine v AD Kreiranje novega posebnega uporabniškega računa Omogočanje uporabniškega računa Onemogočanje uporabniškega računa
Skrbniki računalnikov	Kreiranje novega računalnika v AD
Odobritelji	Odobritev poštnega naslova in domače mape
Vsi zaposleni	Zahteva za članstvo v skupini v AD Zahteva za zamenjavo gesla

Slika 21: Povezava FIM, OIM in ostalih sistemov



3.2.4.5 Okolje in varnost delovanja sistema

Sistem bo živel v okolju, za katerega predpostavimo naslednje:

- uporabniki delajo v pisarnah,
- strežniki bodo v sistemskem prostoru Sektorja za ITT.

Sistem za svoje delo ne potrebuje posebnih pogojev. Potrebovali bomo FIM strežnik in

OIM strežnik ter strežnik za bazo podatkov. Za vse tri so dovolj strežniki po Krkinih standardih. Sistem bo imel razvojno, testno in produkcijsko okolje. Vsa tri okolja bodo na Krkini opremi. Razvojni sistem je namenjen vse spremembam – nastavitvam sistema. Testni sistem je namenjen testiranju sprememb. Produkcijski sistem je namenjen normalni, dnevni uporabi sistema. Vse spremembe sistema se opravi na razvojnem sistemu in pred prenosom na produkcijsko okolje testira na testnem sistemu, kar od Krke zahtevajo tudi razni standardi.

3.2.4.6 Sistem avtorizacij (postopki)

V sistemu bodo za uporabnike definirane različne vloge. Skrbnik sistema bo uporabniku dodelil vlogo na osnovi obrazca, na katerem bodo:

- osnovni podatki o uporabniku,
- podatki o vlogi,
- odobritev vodje,
- odobritev lastnika vloge.

3.2.4.7 Omejitve sistema

Prenos podatkov iz aktivnega imenika v sistem OIM (in kasneje tudi obratno, vendar ne v prvi fazi projekta). Ti podatki bodo obstajali v obeh sistemih. Podatki so:

- uporabniška imena,
- računalniki in
- skupine.

Ocena količine podatkov:

- uporabniška imena nekje 5.000 ~ 8.000,
- računalniki 3.000 ~ 5.000 in
- skupine 1.000.

3.2.4.8 Dokumentacija sistema

Ob vpeljavi sistema je potrebno izdelati tudi tehnično in uporabniško dokumentacijo:

- vzpostavitevni dokument projekta,
- uporabniške zahteve,
- funkcionalna specifikacija,
- dizajn specifikacija,
- postopki:
 - instalacijski in konfiguracijski postopki,
 - operativni (navodila za uporabnike),
 - postopki za upravljanje (navodila za vzdrževalce sistema),
 - načrt varovanja podatkov (*Backup / Restore* postopki),
 - priprava testnih postopkov in pomoč pri izvedbi.

Podatki iz sistema se morajo po prenehanju uporabe hraniti 10 let. Dokumentacija se hrani v projektni mapi (fizično) in na spletnem mestu projekta (elektronsko).

3.3 Možnosti in strategija vpeljave sistema upravljanja identitet

V prejšnjem poglavju sem predstavil podrobne uporabniške zahteve, kot jih pripravi projektna ekipa in na osnovi uporabniških zahtev pridobi ponudbe dobaviteljev. Poleg uporabniških zahtev pa je ključnega pomena tudi spoštovanje standardov, po katerih mora delovati Krka. Farmacevtska industrija je močno podvržena standardizacijam in kontrolam standardov predvsem zaradi narave izdelkov, ki so po večini zdravila. Tudi sami postopki izvajanja opravil v sektorju informatike in telekomunikacij so v veliki meri diktirani prav po izbranih standardih. V največji meri se ITT v Krki drži metodologije ITIL in posledično iz branže farmacevtov tudi GMP regulative. V zadnjem letu še posebnih priporočil za FDA⁸. Za boljše razumevanje načina vpeljevanja projekta upravljanja identitet v nadaljevanju bom na kratko predstavil metodologije in standarde, ki pogojujejo strategijo vpeljave projekta v Krko.

3.3.1 Metodologija ITIL

Information Technology Infrastructure Library (v nadaljevanju ITIL) je skupek konceptov in tehnik za upravljanje informacijske tehnologije (v nadaljevanju IT), infrastrukture, razvoja in operacij. ITIL je objavljen kot serija knjig, od katerih vsaka pokriva določeno temo pri upravljanju IT. Imena ITIL in IT Infrastructure Library sta zaščiteni znamki OGC (angl. *Office of Government Commerce*). ITIL ponuja podroben opis številnih pomembnih

8 FDA je kratica za Food and Drug Administration

postopkov v IT. To je podprto s številnimi izčrpnimi opisi, seznamami in postopki, ki so lahko prilagojeni katerikoli IT organizaciji. Ti opisi in postopki izvirajo iz najboljših praks upravljanja s storitvami. Te metode so zbrane tako z gospodarskega področja kot tudi iz področja negospodarstva. ITIL je v osnovi namenjen vsem, ki se ukvarjajo z IT storitvami. Namen je tudi, da bi bili čim bolj uspešni pri upravljanju IT, hkrati pa imeli podroben vpogled v procese, ki jih uporabljajo pri svojem delu. Glavno sporočilo ITIL je v tem, da so IT storitve namenjene izključno podpori poslovanja in njihovem uspešnem in učinkovitem delovanju. ITIL lahko uporabljajo vse IT organizacije, ne glede na njihovo velikost ali tehnologijo, ki jo pri svojem delu uporabljajo.

Metodologija ITIL ima zaradi svoje zasnove odločilne prednosti pred podobnimi metodologijami. Namreč, njen razvoj je temeljil na tem, da poleg nekih teoretičnih vsebin zajema še dodatne podporne oziroma dopolnilne storitve, ki so podlaga za poslovno področje. Pod te dopolnilne storitve uvrščamo:

- izobraževanje ter usposabljanje,
- sistem certificiranja znanja,
- uporabniško pomoč in druge svetovalne storitve,
- programska orodja, ki so v pomoč pri uvajanju ali izvajanju ITIL,
- združenja in društva na IT področju.

ITIL zbirka in njeni moduli tvorijo okvir (slika 22), ki vsebuje najpomembnejša področja oziroma poslovne procese na IT področju.

Pri ITIL metodologiji sta osrednji področji upravljanja zagotavljanje storitev in podpora storitvam. Zagotavljanje storitev ureja področje (proces), ki je potrebno za kakovostno načrtovanje in zagotavljanje IT storitev. Dolgoročno se ukvarja s tem, da procesi čim bolj izboljšujejo kakovost storitev IT. Pri podpori storitvam gre predvsem za vsakodnevne procese, kot so uporabniška podpora in vzdrževanje IT storitev.

Načrtovanje implementacije upravljanja storitev se ukvarja z načrtovanjem, implementacijo in izboljševanjem procesov upravljanja storitev v neki organizaciji. Poleg tega rešuje zadeve, ki so povezane z organizacijskimi spremembami, razvojem strategije in vizije in najustreznejšo metodo dostopa. Z opisom upravljanja aplikacij od začetnih poslovnih potreb do končne faze (cel življenjski cikel) se ukvarja področje upravljanja aplikacij. Tukaj je zelo pomembno zagotoviti povezanost strategij IT s poslovnimi strategijami, da je poslovanju omogočen kar najboljši izkoristek naložbe v neko aplikacijo. Nasvete in smernice zaposlenim na IT področju razlaga poslovna perspektiva. Svetuje, kako lahko prispevajo k poslovnim ciljem ter kako čim bolje uskladiti in uporabiti vloge in storitve, da bi bil prispevek k poslovnim ciljem čim večji. Upravljanje varnosti obravnava

podrobne postopke načrtovanja in upravljanja varnosti za IT storitve in informacije. To vključuje tudi odzive na varnostne incidente, ocenjevanje tveganja in možnosti varnostnih zlorab, kot tudi stroškovno pripravo upravičenosti protiukrepov. Za upravljanje področij, ki ne tvorijo jedro ITIL okvirja, je pred upravljanjem potrebno zagotoviti, da se osnovne storitve upravljajo na ustreznem nivoju.

Slika 22 : Okvir zbirke ITIL



Vir: Foundations of IT Service Management, based on ITIL, 2006

Upravljanje IT področja mora biti usklajeno s poslovnim modelom organizacije. Upoštevati pa vendarle mora tehnološke zmožnosti in pričakovanja uporabnikov. Da bo IT področje prispevalo k dodani vrednosti poslovanja organizacije, mora vodstvo organizacije zelo natančno ugotoviti in opredeliti vlogo informacijske tehnologije v organizaciji. Ko je ta vloga poznana in odobrena s strani vodstva, lahko IT zagotavlja kakovostne storitve, ki so v pričakovanem poslovnem in finančnem okvirju.

Pri metodologiji ITIL je velik poudarek na različnih vidikih IT (storitve, procesi, organizacija, tehnologija ...) ter povezave IT s celotnim poslovanjem organizacije. Pri uvajanju ITIL metodologije je potrebno pogledati uporabo iz poslovne perspektive. Torej je potrebno preveriti, kakšne prednosti bo imela organizacija od uvedbe metodologije ITIL.

S poslovne perspektive so cilji uvedbe ITIL:

- usklajevanje IT tehnologije s poslovanjem;
- vpeljevanje, vplivanje in omogočanje sprememb vse s ciljem povečanja

konkurenčnosti;

- zaposlenim v IT omogočiti, da razume njihov prispevek k poslovnim ciljem;
- zaposlenim v IT omogočiti razumevanje, da z zagotavljanjem in izboljševanjem IT storitev podpre poslovne cilje in
- zaposlenim v IT omogočiti, da z izrabo informacijske tehnologije pomaga poslovanju.

Uspešni procesi zagotavljajo usklajenost IT storitev z zahtevami poslovanja. Hkrati mora biti ta usklajenost podprta tudi s strani zunanjih dobaviteljev.

Koristi IT organizacije pri uvedbi ITIL-a se kažejo tudi v izboljšanem upravljanju in nadzoru nad spremembami v IT. Izboljša se razpoložljivost, zanesljivost in varnost kritičnih IT storitev. Zmanjšujejo se IT stroški, povečujejo se učinkovitost in ekonomičnost. Organiziranost IT je sistematična in s tem bolj pregledna, saj se zmanjšuje podvajanje dela, procedure pa so standardne in jasne, kar vpliva tudi na zmanjševanje prekinitev poslovanja. Izboljšuje se produktivnost zaposlenih ter njihova izkoriščenost.

Koristi, ki jih prinaša ITIL, pa niso vezane samo na podjetje v smislu lastne učinkovitosti in optimizacije, ampak prinašajo dodano vrednost uporabnikom IT storitev. Nekatere od teh koristi se kažejo v stabilnem IT okolju in v dobro dokumentiranih IT storitvah. Povečuje se zaupanje med uporabniki in IT z zagotovljeno kakovostjo uporabe storitev. Zmanjšuje se čas vpeljave novih IT storitev. Glavno korist pa prinaša povečevanje konkurenčne prednosti podjetja.

3.3.2 Dobra proizvodna praksa (GMP) v farmacevtski industriji

Poleg metodologije ITIL, ki predvsem organizira IT dejavnost, pa smo v Krki zaobljubljeni več različnim standardom. Dobra proizvodna praksa – GMP (angl. *Good Manufacturing Practice*, v nadaljevanju GMP) so smernice, ki so za farmacevtsko industrijo nujne in morajo biti del sistema zagotavljanja kakovosti. Določajo pogoje v proizvodnji in kontroli proizvodnje zdravil, ki omogočajo izdelavo zdravila v skladu s specifikacijo kakovosti izdelka, kot je zapisana v dovoljenju za promet ves čas njegovega roka uporabe (Košiček, 2004, str. 16 – 19).

Cilje GMP lahko na kratko opredelimo kot:

- doseči enak nivo kakovosti (vsak izdelek znotraj serije naj bo enako kakovosten, kot tudi v vsaki seriji),
- preprečiti napake, ki vplivajo na kakovost, varnost in učinkovitost izdelka (na primer zdravila) in tako zaščititi uporabnika – bolnika.

Elementi, ki sestavljajo GMP so:

- sistem zagotavljanja kakovosti,
- osebje,
- delovni prostori in oprema,
- dokumentacija,
- proizvodnja in skladiščenje,
- kontrola kakovosti,
- pogodbeni proizvodnja,
- reklamacije in odpoklici,
- notranja presoja.

Sistem zagotavljanja kakovosti vključuje vse procese, ki vplivajo na kakovost izdelka. Osebje predstavlja najpomembnejši element sistema kakovosti, saj človek s svojimi dejanji, pristopom in drugimi osebnostnimi karakteristikami vpliva na kakovost. GMP predpisuje, kako mora biti osebje strokovno usposobljeno, kakšno je ustrezno zdravstveno stanje in higienska osveščenost ter obnašanje itd.

Prostori morajo biti namenski, in sicer skladiščni, proizvodni, kontrolni laboratoriji in pomožni prostori (garderobe, umivalnice, sanitarije, čajne kuhinje itd.), predviden je tudi njihov raspored in način gradnje instalacije. Vsa oprema mora biti namenska, označena, primerna za čiščenje in umerjena. Imeti mora ustrezen status uporabe in čistoče ter obstajati mora ustrezna dokumentacija.

Dokumentacija je bistveni del sistema zagotavljanja kakovosti, saj enolično opredeljuje posamezne segmente projekta in preprečuje napačno razumevanje ustnih dogovorov ter omogoča vpogled v opravljeno delo in sledljivost posameznih korakov. Predpisana je oblika in vsebina obveznih dokumentov, določene odgovorne osebe za izdajo, odobritev in spremembe ter predpisan je tudi sistem razpošiljanja, odpoklica in uničenja oziroma prenehanja veljavnosti dokumenta. Prav tako so tu opisani tudi postopki upravljanja s spremembami. Proizvodnja obsega skladiščenje, izdelavo in pakiranje. Vloga dobre proizvodnje prakse je, na tem mestu, v preprečevanju različnih (tipičnih) napak, ki se pojavljajo pogosto v proizvodnjah farmacevtskega tipa (MNL Limited, 2012; ISPE, 2012).

3.3.3 FDA predpisi

V letu 2011 smo v Krki izvajali intenzivno pripravo na skladnost poslovanja z ameriško FDA regulativo, ker želimo izbrane farmacevtske izdelke prodajati na njihov trg. Regulativa FDA je ena izmed najbolj strogih regulativ in tudi zelo ostro kaznuje podjetja,

ki ne opravijo njihove presoje. Sama prisotnost farmacevta, kot je Krka, na ameriškem tržišču, je zelo prestižna potrditev o dobrem in kvalitetnem delu podjetja, zato si želimo te potrditve, kot tudi same prodaje na omenjenem trgu.

Naslov 21 CFR⁹ Odsek 11 (v nadaljevanju Odsek 11) se ukvarja s smernicami standardizacije FDA o elektronskih zapisih in podpisih v ZDA. Odsek 11 definira kriterij, po katerem naj bi elektronski zapisi in podpisi bili zaupanja vredni in enakovredni papirnim zapisom. Iz prakse sodeč pa Odsek 11 zahteva od proizvajalcev zdravil in medicinskih naprav ter ostalih branž podvrženim FDA, da vpeljejo mehanizme beleženja (*audit*), preverjanja (*validation*), sledljivosti (*audit trail*), elektronskega podpisa ter dokumentacijo za sisteme, ki se uporabljajo neposredno pri proizvodnji presojanega izdelka in neposredno ustvarjajo elektronske zapise o sami proizvodnji. Za le-te je zahtevana sledljivost oziroma kar predpisujejo predikatna pravila (angl. *predicate rules*). Predikatna pravila so katerakoli pravila iz ostalih odsekov FDA priporočil in zahtev, torej je zahtevana skladnost tudi z ostalimi predpisi regulative izven Odseka 11 (FDA predpisi, 2003, str. 4).

V Krki smo predani oblikovanju poslovanja po mednarodnih standardih in priporočilih, kar pa nam nalaga vse več dela s podrobno izdelavo dokumentacije o sistemih, hranjenju elektronskih zapisov o transakcijah sistemov, zapise in poročila zaposlenih o izvedenih delih itd. Vpeljava sistema upravljanja identitet je v svoji zasnovi zelo dober pripomoček za ustvarjanje takih elektronskih zapisov o identitetah, njihovih prehajanjih med posameznimi organizacijskimi enotami, prehajanje med domenskimi skupinami, ki odražajo pravice na sistemih ter druge pomembne zapise, ki jih še predpisuje Odsek 11 in ostala predikatna pravila.

3.4 Postopek vpeljave izbrane rešitve

Postopek vpeljave sistema je v Krki definiran s splošnim operativnim postopkom, ki definira na kakšen način poteka vodenje projekta vpeljave sistema v podjetje. V poglavju bom opredelil postopek vodenja projekta upravljanja identitet v podjetje Krka po interno predpisanih standardih, ki se v večini vežejo in so izpeljani iz standardov, opisanih v poglavju 3.3.

Ne glede na vrsto IT projekta je postopek izvajanja IT projekta, razen v fazi priprave in imenovanja projekta, identičen za vse tipe projektov. Projekt vpeljave sistema upravljanja identitet opredelimo kot IT projekt na nivoju Krke, saj vpleta v realizacijo več oddelkov in služb v podjetju. V prvi fazi projekta, ko se vpeljuje upravljanje uporabnikov in sama

9 CFR je kratica za Code of Federal Regulations, Title 21

sinhronizacija avtoritativnih virov v meta-imenik, sta vključeni službi ITT in kadrovska služba.

Ostali tipi projektov, ki se še izvajajo v okviru tega postopka:

- IT projekti, ki so sestavni del investicijskih projektov Krke,
- samostojni IT projekti SITT,
- IT projekti na nivoju Krke.

3.4.1 Vzpostavitev projekta

V primeru IT projektov na nivoju Krke, v kar sodi tudi projekt vpeljave upravljanja identitet, predlog projekta pripravi lastnik procesa. V predlogu opredeli trenutno stanje procesa, predlog spremembe procesa v okviru projekta, vrsto razloga projekta (optimizacija procesa oziroma skladnost z zakonodajo in standardi), dodano vrednost projekta (izboljšanje) ter kriterije preverjanja uspešnosti projekta.

Projekt upravljanja identitet je opredeljen z vrsto razlogov skladnosti z zakonodajo in standardi z vidika kakovosti, zato mora biti predlog projekta pred posredovanjem v SITT odobren tudi s strani odbora za kakovost. Lastnik procesa predlog posreduje vodji sektorja ITT, ki je dolžan oceniti oziroma pridobiti investicijsko vrednost projekta. Vodja nato na osnovi opredeljene dodane vrednosti projekta, ocene investicijske vrednosti projekta oziroma skladnosti z zakonodajo in standardi ter ob upoštevanju razpoložljivih kapacitet v SITT, potrdi ali zavrne predlog projekta in določi prioriteto projekta. V kolikor predvidena investicijska vrednost presega finančno omejitve vodje sektorja, le-ta posreduje predlog projekta v odobritev upravi družbe oziroma odboru za investicije (postopek je prikazan na sliki 23).

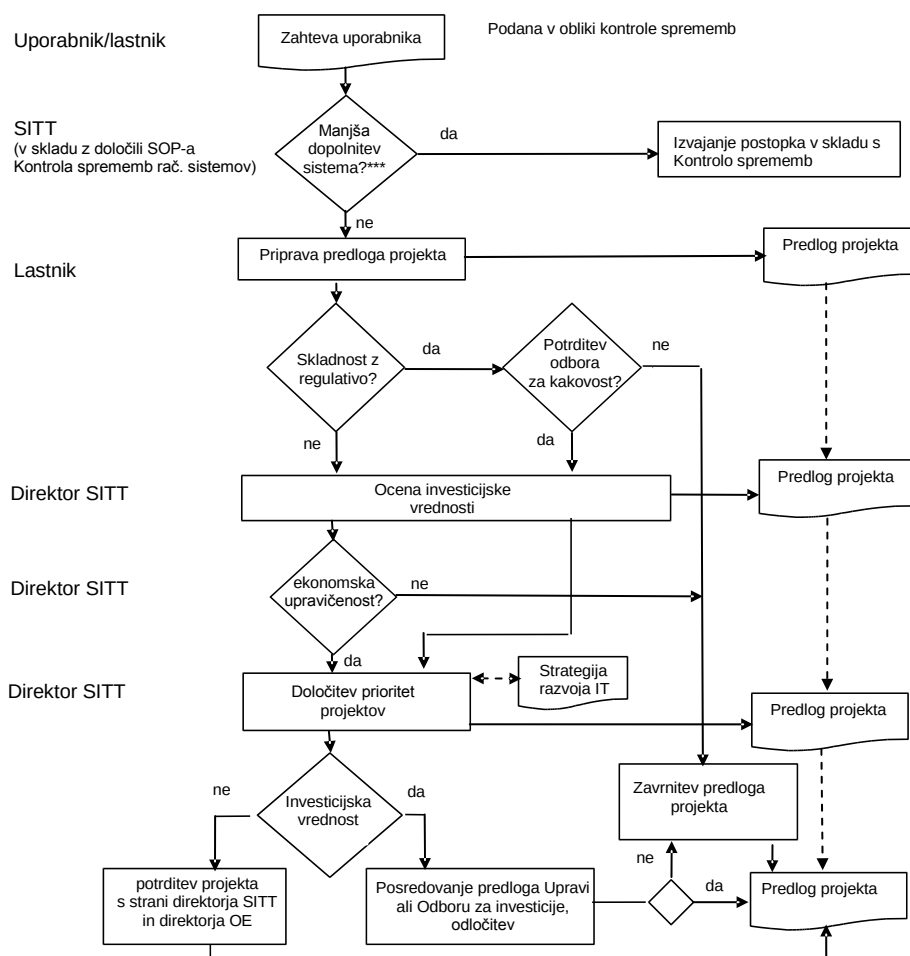
3.4.2 Projektna skupina

Na osnovi odobrenega predloga projekta uprava družbe ali direktor SITT skupaj z vodjo organizacijske enote imenujeta vodjo projekta in ostale člane projektne skupine ter nadzorni svet projekta.

V primeru projekta upravljanja identitet (ali tudi za investicijske projekte Krke) uprava družbe oziroma komisija za investicije praviloma imenuje tudi vodjo projekta s strani uporabnikov, ki za čas trajanja projekta lahko izvaja naloge lastnika procesa/sistema v skladu s pooblastili, ki mu jih le-ta dodeli.

Projektne ekipe projekta upravljanja identitet je prvotno sestavljena iz: vodje projekta na nivoju celotne Krke, vodje projekta s strani IT, vodje projekta s strani uporabnikov, skrbnika sistema KIS, skrbnika sistema SAP HR, skrbnika sistema AD, skrbnika sistema poštnega strežnika in projektne ekipe dobavitelja, ki jo sestavlja: vodja projekta s strani dobavitelja ter strokovnjaki za posamezna področja, ki tehnično implementirajo sistem in agente.

Slika 23: Postopek odobritve IT projekta na nivoju Krke



Vir: Interna dokumentacija Krka

3.4.3 Priprava na izvedbo projekta

V praksi se vsak projekt dejansko prične šele ob vzpostavitvi projektne mape, ki jo pripravi vodja projekta in je namenjena enotnemu mestu za hranjenje projektne dokumentacije. Glede na projektno ekipo je potrebno dodeliti ustrezne pravice članom ekipe za urejanje te

mape ter pripraviti dokument »Vzpostavitevni dokument projekta – VDP«, ki v grobem opredeljuje razloge, zakaj je potrebna vpeljava sistema identitet, kaj so cilji projekta, grob načrt izvedbe projekta v smislu kaj želimo doseči in na kakšen način, grob terminski plan projekta, projektno ekipo in okvirne predvidene stroške.

Na osnovi imenovanja projekta se projektu dodeli projektno številko znotraj sistema vodenja projektov v SITT z referenčno številko na nadrejeni projekt, če le-ta obstaja. Šifra projekta je definirana po internem sistemu šifriranja projektov, kar omogoča hierarhično umestitev projektov.

3.4.4 Priprava uporabniških zahtev

V kolikor gre za investicijske projekte (projekte, ki potrebujejo gradbeno dovoljenje), je nivoju krovnega projekta potrebno pripraviti Tehnološka izhodišča projekta, katerih sestavni del so tudi izhodišča za delovanje IT sistemov/storitev in pripadajoče infrastrukture. Vodja projekta koordinira izdelavo skupaj z lastniki procesa/sistema in z ostalimi člani projektne ekipe.

Za podrobnejšo definicijo potreb delovanja sistema upravljanja identitet projektna ekipa izdelava dokument »Uporabniške zahteve – URS«. Nosilec naloge je lastnik procesa/sistema (oziroma vodja projekta s strani uporabnikov) skupaj z ostalimi člani projektne ekipe. Dokument odobrita vsaj lastnik procesa in vodja projekta ter direktor SITT. Poleg odobritve vodij pa je pogosto potrebna tudi odobritev za sisteme s strani oddelka zagotavljanja kakovosti, ki jih označujemo kot GxP kritične sisteme oziroma sisteme, za katere GMP predvideva posebne predpise, kako jih voditi, kot je bilo to potrebno za sistem upravljanja identitet.

V primeru, ko gre za manjše projekte, ki se ne nanašajo na GxP kritične sisteme, so lahko uporabniške zahteve zapisane v »Vzpostavitevni dokumentu projekta – VDP«, dokument »Uporabniške zahteve – URS« pa ni potreben.

Ker je projekt upravljanja identitet GxP kritičen sistem, je potrebno izdelati tudi t. i. »Validacijski plan projekta – VMP«, kjer projektna ekipa definira potrebne kvalifikacijske aktivnosti v fazi izvajanja projekta. Nosilec naloge za izdelavo validacijskega plana je pooblaščen oseba oddelka zagotavljanja kakovosti.

3.4.5 Izbira dobavitelja

Projekt upravljanja identitet presega obseg realizacije z zaposlenim kadrom, zato se

pristopi k izbiri zunanjega dobavitelja sistema. Pri zunanjih dobaviteljih za GxP kritične sisteme se izvaja presoja sistema kakovosti dobavitelja oziroma se pridobi zapisnik o presoji s strani pooblaščen organizacije. Presoje dobaviteljev so s strani Krke zelo dobrodošle, saj bistveno olajšajo izvedbo del z dobavitelji, ker le-ti poznajo sistem kakovosti v Krki in tako lažje pripravljajo ustrezno dokumentacijo skozi projekt, ki odgovarja prej omenjenim standardom.

Z izbranim dobaviteljem se nato pripravi pogodba za izvedbo del, kjer se natančno specificira obseg del, dokumentacija ter časovni okvir projekta. Za koordinacijo aktivnosti in izdelavo podrobnega terminskega plana je zadolžen vodja projekta.

3.4.6 Priprava funkcionalne in dizajn specifikacije

Izbrani dobavitelj v sodelovanju s projektno ekipo na osnovi uporabniških zahtev pripravi funkcionalno (tehnični opis izvedbe) in dizajn (logični načrt) specifikacijo sistema – FS in DS.

Del funkcionalne in dizajn specifikacije mora biti tudi matrika sledljivosti, ki omogoča povezavo med uporabniškimi zahtevami in funkcionalno oziroma dizajn specifikacijo. Kot sem omenil že prej, je dokument funkcionalne in dizajn specifikacije (ki je lahko en sam dokument, kar je tudi pogosta praksa) dejansko odgovor na uporabniške zahteve in je razdelan po enakih postavkah kot sam URS. Vključevanje tehnične podrobnosti o izvedbi rešitve bi preseglo obseg te naloge ter hkrati prikazalo samo tehnični odgovor na URS pri uporabi določenega sistema upravljanja identitet. Odobritev funkcionalne in dizajn specifikacije opravijo iste osebe kot odobritev uporabniških zahtev.

S tem se tudi zaključi faza priprave uvodne dokumentacije. Projektna ekipa tako dobi podroben načrt izvedbe projekta. Kot sem omenil v uporabniških zahtevah, je posegov v druge sisteme malo, v večini primerov se sisteme uporabi kot avtoritativne vire podatkov, aktivni imenik pa postane sistem, v katerega se sinhronizirajo ti podatki, saj ima Windows okolje za potrebe prve faze projekta vgrajene mehanizme avtentikacije in avtorizacije za povezane sisteme. Upravljanje uporabniških vlog na povezanih sistemih pa poteka skozi upravljanje domenskih skupin.

3.4.7 Izvedba projekta

Izbrani dobavitelj sistema in projektna ekipa na osnovi odobrenih dokumentov in pripravljene rešitve pričneta s postavitvijo razvojnega okolja, kjer se najprej namestijo potrebni sistemi in agenti, ki bodo skrbeli za sinhronizacijo. Vpeljanih je bilo nekaj novih strežnikov, ki si delijo funkcionalnosti meta-imenika, sinhronizacijskega strežnika z agenti

in strežnika z uporabniškim vmesnikom (spletni vmesnik).

Na razvojnem sistemu se opravi tudi konfiguracija sistema, ki je predstavljala večji izziv vpeljave, saj je bilo potrebno identificirati vse attribute iz posameznih avtoritativnih virov (KIS in SAP HR) ter jih preslikati v sistem IdM. Sistem smo v našem primeru sestavili iz dveh produktov, kjer Microsoft Fore-front Identity Manager skrbi predvsem za *provisioning* oziroma sinhronizacijo tako podatkov različnih virov v meta-imenik, kot tudi upravljanje aktivnega imenika, kjer se dejansko realizirajo zahtevane spremembe na objektih. Druga komponenta pa je *Omada Identity Manager*, ki ponuja zelo kvalitetni spletni uporabniški vmesnik in sam izdelek bazira na FIM-u kot sinhronizacijskem servisu, tako da vsak produkt opravlja eno izmed pomembnih vlog sistema upravljanja identitet.

Ob izvedbi priprave projekta v razvojnem okolju so zaželeni vmesni pregledi opravljenega dela ter vmesna poročila o napredku projekta. Za pripravo vmesnih poročil o napredku je odgovoren vodja projekta in ko je opravljena konfiguracija razvojnega sistema, se projekt preseli v fazo namestitve produkcijskega in testnega okolja.

3.4.8 Namestitev in testiranje

Dobavitelj sistema in projektna ekipa namestita izdelano rešitev na produkcijsko opremo Krke na način, kot je bilo to izvedeno na razvojnem sistemu. Namestitve na razvojnem sistemu služijo kot faza, v kateri se tudi pripravi kvalifikacijske zapisnike in navodila, ki se uporabijo pri izvedbi na produkcijsko okolje. Za razliko od razvojnega okolja postopek namestitve produkcijskega okolja teče po vnaprej določenih korakih in hkrati zahteva izdelavo kvalifikacijskega poročila, ki smo ga vnaprej pripravili. Postopki morajo biti skladni s postopkom izvajanja instalacij in konfiguracij IT sistemov, kot je to opredeljeno v internih standardih podjetja.

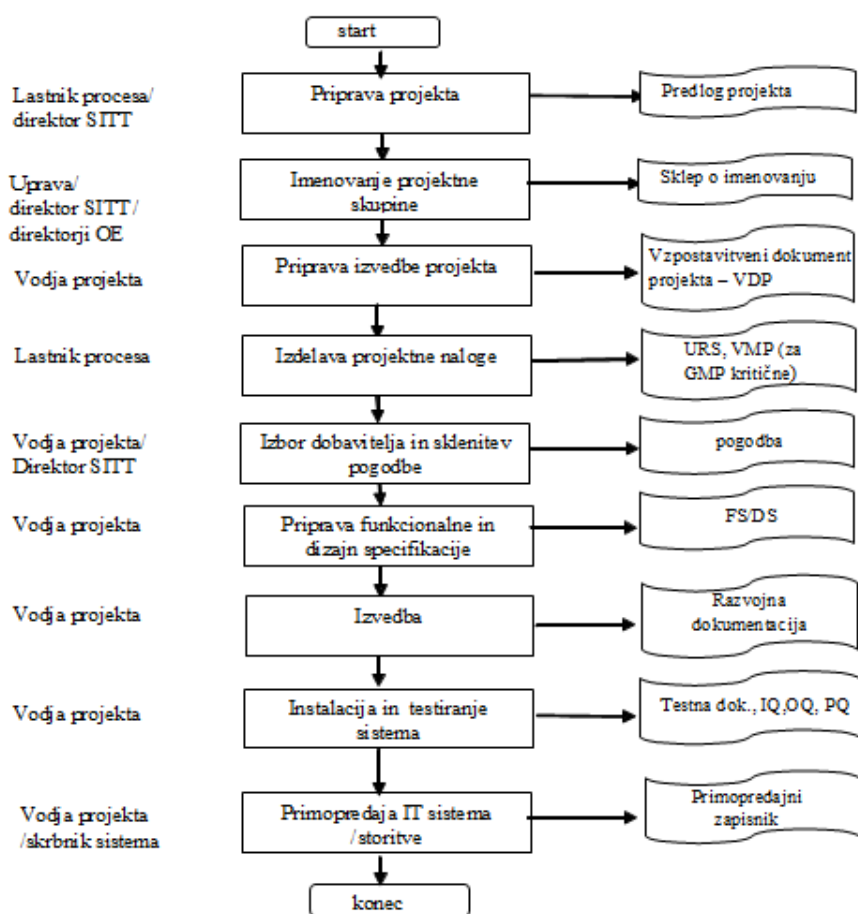
Testni sistemi se navadno postavijo tako, da se postavljeno produkcijsko okolje preslika v testno okolje, če je to možno oziroma se izvede enak postopek namestitve kot na produkcijskem sistemu. Testni sistemi so v celoti ločeni od produkcijskih, torej imajo ločene tudi podatke. Projekt upravljanja identitet pa neposredno upravlja z aktivnim imenikom v podjetju, katerega testno okolje, ki ni popolnoma fizično ločeno od produkcijskega, ne more obstajati zaradi tehničnih lastnosti aktivnega imenika. Postavitev fizično ločenega testnega okolja smo dosegli z replikacijo izbranih produkcijskih strežnikov v ločeno virtualno okolje, kjer smo dejansko lahko testirali vse funkcionalnosti na dejanski kopiji podatkov aktivnega imenika in ne samo za vnaprej pripravljene testne podatke. Testiranje rešitve je sledilo v skladu s postopkom testiranja IT sistemov.

Po uspešni namestitvi in izvedenih kvalifikacijskih testih se zaključi faza izvedbe. Potrebna je še operativna kvalifikacija delovanja sistema (angl. *Operational Qualification – OQ*), ki potrdi še funkcionalnost sistema.

3.4.9 Primopredaja sistema

Dobavitelj pripravi sistem in dokumentacijo za primopredajo sistema na osnovi pogodbe. Primopredaja s strani Krke obsega vsaj testiranje (oziroma pregled dokumentacije o testiranju) izdelanih rešitev ter pregled celotne dokumentacije sistema (zahteve, specifikacije, navodila itd.) Ker je projekt upravljanja identitet GxP kritični sistem, je potrebno izvesti vse aktivnosti, ki so zahtevane v validacijskem planu projekta (VMP) in vključujejo validacijo vseh komponent sistema. Po končanem testiranju oziroma pregledu dokumentacije vodja projekta skupaj z dobaviteljem sistema pripravi primopredajni zapisnik.

Slika 24: Shema postopka



Vir: Interna dokumentacija Krka

V primeru, da skrbnik IT sistema/storitve ni član projektne ekipe, je potrebno opraviti primopredajo tudi med vodjo projekta in skrbnikom IT sistema/storitve, saj skrbnik tehnično vzdržuje sistem v življenjskem ciklu.

Vodja projekta je dolžan projektno dokumentacijo celostno pripraviti za prenos v arhiv izvedenih projektov ter v mapi IT sistemov/storitev pripraviti krovno mapo z zadnjimi verzijami dokumentov, ki služijo kot operativna dokumentacija sistema/storitve.

3.4.10 Uporaba sistema

Sistem je ob opravljeni primopredaji pripravljen na uporabo v produkcijskem okolju podjetja. Usposobljeni so že vsi kadri, ki bodo operativno izvajali dela na sistemu upravljanja identitet. Ob primopredaji oziroma zaključku projekta vodja sektorja ITT sistem/storitev zavede v katalog sistemov in določi lastnika in skrbnika IT sistema/storitve. Projekt dobi status »zaključen«.

Slika 24 prikazuje postopek vodenja projekta shematično z opisi faz in akcij na desni. Vsi koraki so obvezni za GxP kritične sisteme in projekte. V Krki praktično vse projekte izvajamo z zunanjimi dobavitelji, le nekaj izjem je izvedenih interno brez pomoči dobaviteljev.

3.4.11 Opredelitev odgovornosti med izvajanjem projekta

Spodnja tabela povzema in prikazuje odgovornosti posameznikov, vključenih v projekt. Odgovornosti v posameznih korakih sem opisal že v samih korakih, sedaj pa podajam še konsolidiran pregled odgovornosti v tabeli 6.

Tabela 6: Odgovornosti pri projektu

Naloga	Vodi	Izvaža	Odobri
Priprava projekta	Lastnik procesa	-	Vodja SITT, uprava družbe
Imenovanje članov projektne skupine	Uprava/vodja SITT/Odbor za investicije	Uprava/vodja SITT/Odbor za investicije	Uprava / vodja SITT
Priprava izvedbe IT projekta	Vodja projekta	Člani projektne ekipe	Svet projekta/vodja SITT/vodje služb v SITT

se nadaljuje

Naloga	Vodi	Izvoja	Odobri
Izdelava projektne naloge	Lastnik procesa	uporabniki/vodja projekta/člani projektne skupine/Služba zagotavljanja kakovosti	Vodja projekta/lastnik procesa/direktor SITT / Odbor za kakovost
Izbor dobavitelja in sklenitev pogodbe za izvedbo	Vodja projekta	Člani projektne skupine/vodje služb v SITT	Svet projekta/direktor SITT
Priprava funkcionalne in dizajn specifikacije	Vodja projekta	Izbrani dobavitelj/člani projektne skupine	Lastnik procesa/Vodja projekta/Odbor za kakovost
Izvedba	Vodja projekta	Izbrani dobavitelj/člani projektne skupine	Vodja projekta/Lastnik procesa/Odbor za kakovost
Instalacija in testiranje sistema	Vodja projekta	Člani projektne skupine	Vodja projekta/Lastnik procesa/direktor SITT/Odbor za kakovost
Primopredaja IT sistema/storitve	Vodja projekta	Vodja projekta/lastnik procesa/skrbnik IT sistema	Svet projekta/direktor SITT/vodje služb v SITT

Vir: Interna dokumentacija Krka

3.4.12 Dokumentacija za potrditev kontrol izvajanja postopka

Dokumenti, potrebni za potrditev kontrol izvajanja postopka, ki jih pripravi projektna skupina tekom projekta, so:

- sklep o imenovanju članov projektne skupine,
- vzpostavitevni dokument projekta – VDP,
- projektna dokumentacija (URS, DS, FS, IQ, OQ, PQ),
- zapisniki sestankov in
- primopredajni zapisnik.

3.4.13 Izvedba kvalifikacije sistema upravljanja identitet

Vpeljan sistem upravljanja identitet je klasificiran kot IT sistem in kot tak mora spoštovati pravila validacij za IT sisteme. Validacije in kvalifikacije se izvajajo v skladu z izhodišči GMP ter internimi smernicami Sektorja za upravljanje kakovosti oziroma Službe za tehnološko-tehnično zagotavljanje kakovosti in za validacije. Kvalifikacijski cikel se prične s prepoznavanjem sistema, ki se bo kvalificiral in nadaljuje z zapisom uporabniških

zahtev. Življenjski cikel nato poteka skozi pripravo na izgradnjo, izvedbo analize tveganj, skozi samo izgradnjo, testiranja, primopredaje – prevzema sistema, vzdrževanja sistema v kvalificiranem stanju in njegove ukinitve. Podroben način kvalifikacije je definiran v Validacijskem planu projekta (VMP).

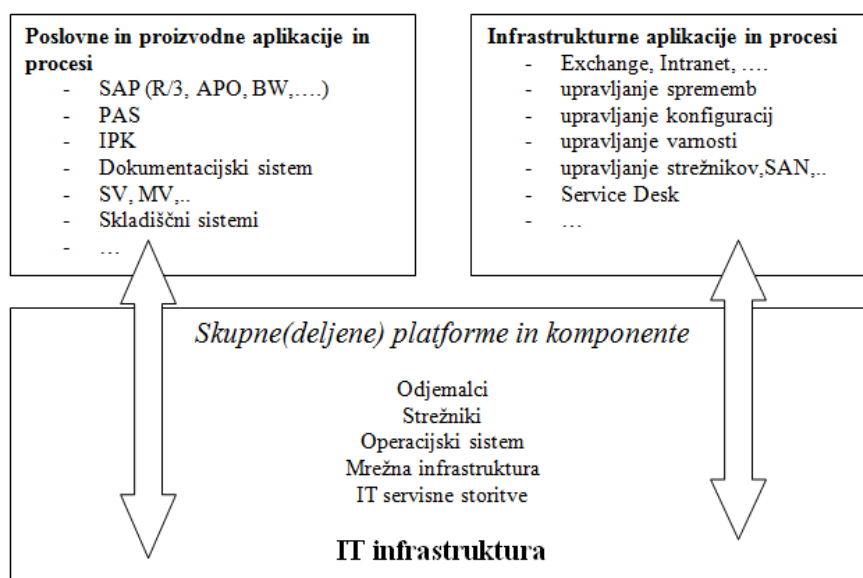
Sistem kvalifikacije je ključni korak pri zagotavljanju tako pravilnosti namestitve, pravilnosti delovanja in produkcijskega delovanja sistema v podjetju. V nadaljevanju bom predstavil, kako smo validirali sistem upravljanja identitet in kako v splošnem validiramo sisteme v Krki.

3.4.14 Ključni elementi sistema upravljanja infrastrukture

Ključni elementi infrastrukture morajo biti definirani jasno in enolično. Vsi sistemi (vključno s sistemom upravljanja identitet) morajo uporabljati tipske infrastrukturne elemente, ki so vnaprej definirani. Le-ti so združeni v platformah, ki jih zaposleni (ljudje) obvladujejo preko definiranih procesov:

- platform,
- procesov in
- odgovornosti.

Slika 25: Horizontalni pristop kvalifikacij



Vir: Interna dokumentacija Krka

Platforme. Platforme so standardni sklopi infrastrukturne opreme (komponent), ki so osnova za postavitev višje ležečih zahtev.

S prepoznavanjem standardnih platform zmanjšamo obseg dokumentiranega testiranja novih sistemov. Princip je zasnovan na načelu, da različni tipi komponent zahtevajo različne pristope h kvalifikaciji. Podobne komponente pa imajo enake osnovne zahteve za doseganje kvalificiranega stanja. Obseg potrebnih kvalifikacij prikazuje slika 25. Definicija vseh potrebnih kvalifikacijskih aktivnosti za posamezno komponento pa je odvisna od kategorizacije komponent v infrastrukturnih nivojih ter od GAMP kategorije, kot prikazuje tabela 7.

Tabela 7: Obseg kvalifikacij

Infrastrukturni nivo komponent	Minimalne zahteve za nadzor	GAMP
Ožičenje	Načrti ožičenja z detajli (patch paneli, oznake,...) Merjenje in spremljanje fizičnih povezav	1
Strojna oprema (mrežne kartice, napajalniki, tiskalniki, ...)	Upravljanje inventarja in shranjevanje konfiguracij (enota, lokacija in identifikacija v načrtu, stalen monitoring performans)	1
Mrežne naprave	Upravljanje inventarja in shranjevanje konfiguracij (enota, lokacija in identifikacija v načrtu, stalen monitoring performans)	2
Mrežne storitve (DHCP, ...)	Upravljanje konfiguracij storitev (licence, ...) Kontrola sprememb, monitoring performans	1
Strežniki	Upravljanje inventarja in shranjevanje konfiguracij (enota, lokacija in identifikacija v načrtu, stalen monitoring performans, kontrola sprememb)	0, 1
Operacijski sistem	Upravljanje inventarja in shranjevanje konfiguracij Kontrola sprememb Stalen monitoring, event logging	0, 1
Firmware	Upravljanje inventarja in shranjevanje konfiguracij Kontrola sprememb event logging	0, 1
Infrastrukturne aplikacije (e-mail, PS, FS, web servisi, SMS, MSMQ, ...)	Kontrola sprememb Stalen monitoring, event logging	0, 1, 2

se nadaljuje

Infrastrukturni nivo komponent	Minimalne zahteve za nadzor	GAMP
Namizni odjemalci	Upravljanje inventarja in shranjevanje konfiguracij Kontrola sprememb Stalen monitoring, event logging	1, 2
IT servisne storitve	Kontrola sprememb Stalen monitoring, event logging	3, 4
Aplikacije	Kontrola sprememb Stalen monitoring, event logging	3, 4

Vir: Interna dokumentacija Krka

Procesi v postopku kvalifikacij. Procesi, ki nastopajo pri obvladovanju postopka kvalifikacij informacijske infrastrukture, so:

- proces Nadzora/izbire dobaviteljev;
- proces Upravljanje delovanja (strežnikov/odjemalcev/mreže);
- proces Upravljanje varnosti (zaupnost, integriteta, razpoložljivost);
- proces Izdelovanja varnostnih kopij, Restavriranje in Arhiviranje;
- proces *Disaster Recovery* (reduciranje izpada kritičnih poslovnih funkcij kot posledice incidenta, na sprejemljiv nivo);
- proces *Help desk*, Upravljanje incidentov in problemov;
- proces Kontrole sprememb po implementaciji sistema;
- proces Upravljanje konfiguracij po implementaciji sistema;
- proces spremljanja sistemov (angl. *Performance Monitoring*) (predvsem razpoložljivost in odzivnost);
- proces Periodičnega pregleda sistemov.

Vsi procesi morajo biti pokriti s pripadajočimi dokumenti, ki so t. i. Standarni operativni postopki v Krki in opišejo potek procesa.

Odgovornosti v postopku kvalifikacij. Odgovornosti zaposlenih in vloge, ki nastopajo pri obvladovanju postopka kvalifikacij informacijske infrastrukture, so:

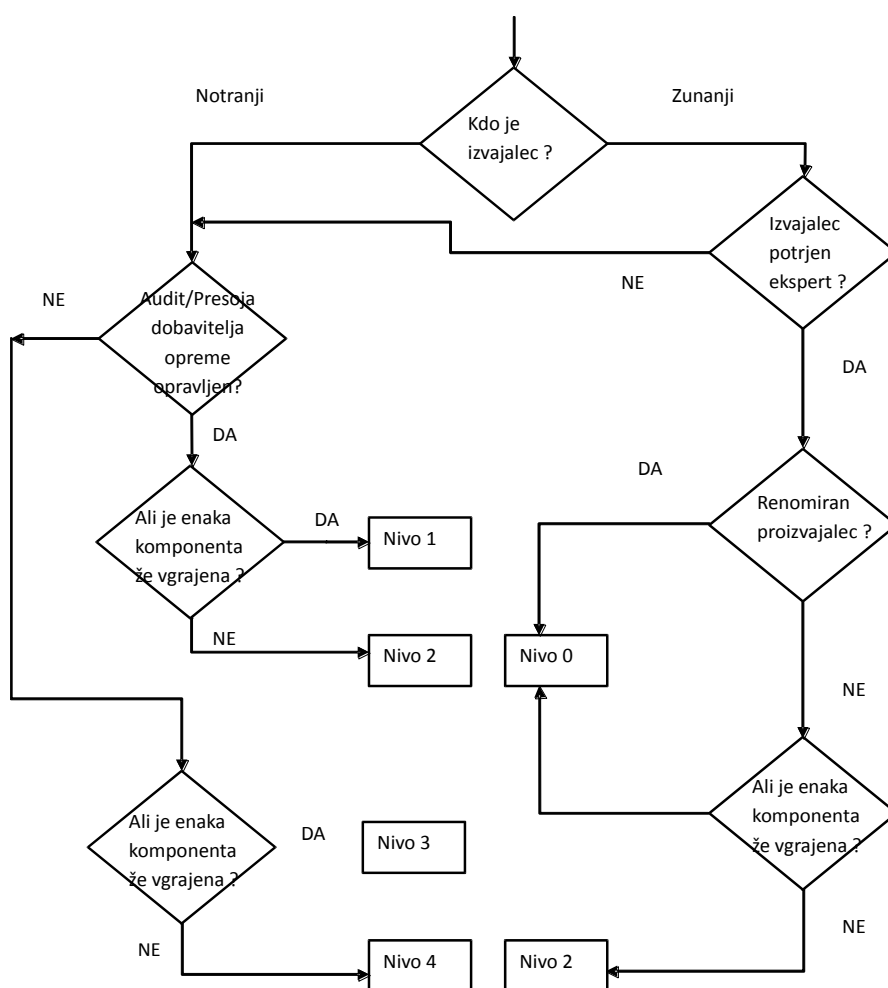
- IT vodstvo/lastnik infrastrukture: sponzor projektov, definiranje splošnih zahtev, ugotovitev sprejemljivega nivoja tveganja, odgovornost za obvladovanje vseh procesov v obvladovanju informacijske infrastrukture,
- projektni vodje vodijo vse projektne aktivnosti,
- skrbniki infrastrukturnih sistemov (platform) določijo zahteve za sistem, skrbijo za delovanje sistema skladno z dogovorom,

- skrbniki sistemov (aplikacij) določijo zahteve za sistem (aplikacijo), skrbijo za delovanje sistemov (aplikacij) skladno z zahtevami,
- ostali IT strokovnjaki in tehnično osebje sodelujejo na projektih in operativnem delu ter izvedbi kvalifikacijskih aktivnosti,
- predstavnik zagotavljanja kakovosti presoja skladnosti z GxP zahtevami in standardi podjetja.

3.5 Postopek kvalifikacije sistema

Na podlagi definiranega nivoja kvalifikacij, minimalnega zahtevanega obsega specifikacij in testov (glej tabelo 7) ter ocene tveganja se definira plan potrebnih kvalifikacijskih aktivnosti.

Slika 26: Izdelava plana kvalifikacij



Vir: Interna dokumentacija Krka

- Osnova za obseg kvalifikacij je tabela 5, kjer je opredeljen obseg zahtevane dokumentacije, obseg testiranja in obseg nadzora.
- Na osnovi ocene tveganj se ugotovi ali so potrebni dodatni ukrepi iz tega naslova. Če so potrebni dodatni ukrepi, se le-te izvede ter sorazmerno s spremembami predpiše dodatne kvalifikacijske aktivnosti (dokumentacija, IQ testi, OQ testi), ki preverijo pravilnost delovanja spremenjenih funkcionalnosti. V kolikor ni potrebnih dodatnih ukrepov za zmanjšanje tveganj, tudi niso potrebne dodatne aktivnosti iz naslova ocene tveganj.
- Obseg kvalifikacijskih aktivnosti se dopolni še z aktivnostmi glede na kvaliteto, strokovnost in zanesljivost dobavitelja.

Kvalificirati je potrebno vse infrastrukturne komponente, platforme ali sisteme, ki so osnova za delovanje sistemov (aplikacij) ali imajo lahko kakršenkoli vpliv na delovanje sistemov (aplikacij). Možnost vpliva in velikost vpliva se ugotovi na osnovi ocene tveganj sistema in povezanih sistemov, ki so predmet kvalifikacije.

Ker kvalifikacijske aktivnosti niso odvisne samo od kategorije komponent, moramo definirati tudi obseg in zahtevnost aktivnosti, ki izhajajo iz zanesljivosti komponent, kvalitete dobavitelja in strokovnosti izvajalca.

Postopek izvajanja kvalifikacije je prikazan v sliki 26 in v tabeli 8 so prikazane še dodatne aktivnosti, ki so potrebne:

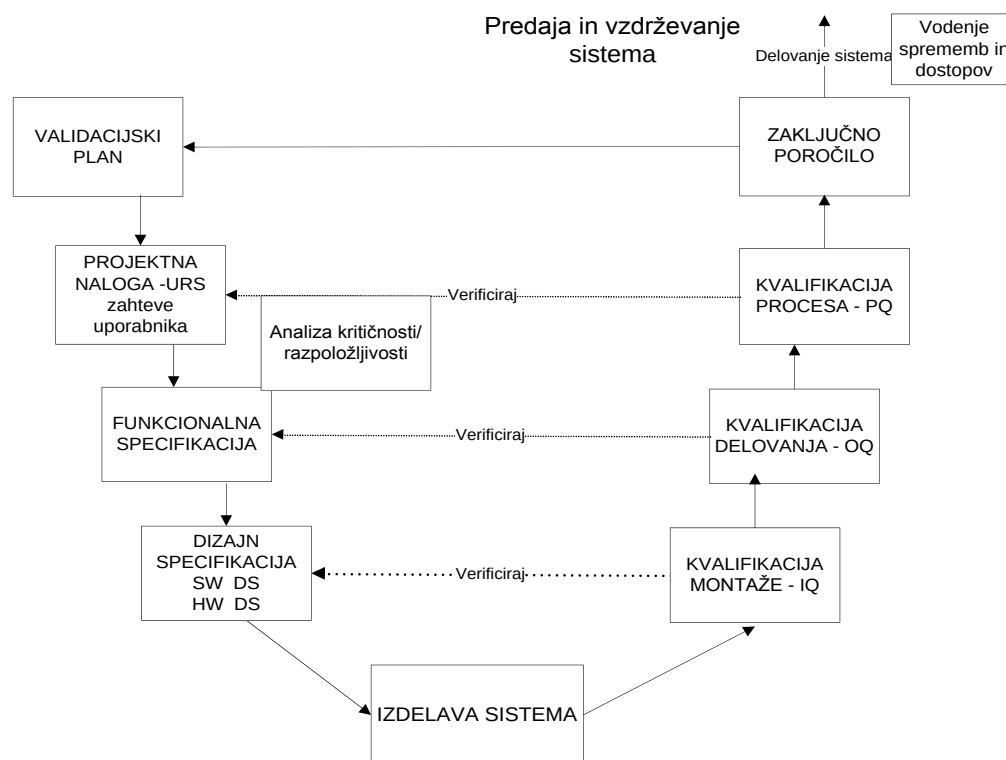
Tabela 8: Določevanje dodatnih aktivnosti na osnovi postopka

Nivo	Potrebne dodatne aktivnosti
0	Zagotoviti je potrebno zahtevam iz tabele 7. Izvajalec implementacije opravlja tudi testne aktivnosti, ter po dogovoru lahko tudi dobavi zahteve iz področja nadzora. Zaželeno je tudi evidenca, ki dokumentira presojo izvajalca ali njegovo ekspertnost.
1	Izvajalec mora izvesti skladno z zahtevami iz tabele 7. Zahtevana je tudi evidenca, ki dokumentira presojo izvajalca ali njegovo ekspertnost.
2	Skladno z zahtevami iz tabele 7 in nivoja 1. Poleg tega še dokumentiran dokaz kvalitete ali splošne uporabe teh komponent v industriji. Če gre za nove, nepreverjene komponente se upošteva nivo 4.
3	Skladno z zahtevami iz tabele 7. Zahtevan audit izvajalca. Glede na rezultat presoje se lahko zahtevajo še dodatne kvalifikacijske aktivnosti upoštevajoč oceno tveganja.
4	Skladno z zahtevami iz tabele 7 in nivoja 3. Obvezne dodatne kvalifikacijske aktivnosti glede na oceno tveganja uporabe nestandardnih komponent.

Vir: Interna dokumentacija Krka

3.5.1 Življenjski cikel kvalifikacije sistema

Slika 27: Življenjski cikel kvalifikacije sistema – V model



Vir: Interna dokumentacija Krka

Življenjski cikel kvalifikacije lahko obravnavamo kot lastni sistem, čeprav je enak vsem projektom na enakem nivoju (tip projekta in sistema). GMP predpisuje kvalificiranje po t. i. V modelu, ki je prikazan v sliki 27. Sam potek življenjskega cikla kvalifikacij bom opisal v naslednjih podglavjih.

3.5.2 Dokumentacija kvalifikacije sistema

Vsaka kvalifikacija predvideva presojanje po pripravljenih dokumentih projekta oziroma sistema. Projektna dokumentacija je, kot sem omenil prej, urejena v **krovni mapi** sistema, ki vsebuje razlago sistema in določa strukturo dokumentaciji. Dokumenti v modelu kvalifikacije so razdeljeni vsebinsko in kategorično glede na GAMP nivo:

- plan validacij (angl. *Validation Master Plan*), (GAMP nivo 3,4);
- uporabniške zahteve (URS), GAMP nivo (2, 3, 4), Interni standardi, navodila za instalacijo, specifikacija konfiguracij, GAMP nivo (0, 1);
- presoja dobavitelja (novih dobaviteljev, oziroma novih platform);
- funkcionalna specifikacija (Functional Specification – FS in GAMP nivo 3,4);

- design specifikacija (Design Specification – DS in GAMP nivo 3, 4);
- kvalifikacija namestitve – IQ (Installation Qualification, GAMP nivo 0, 1, 2, 3, 4);
- kvalifikacija delovanja – OQ (Operational Qualification) in GAMP nivo 2, 3, 4);
- zaključna poročila sistema (projekt);
- zapisnik o izvedenem šolanju;
- Občasni pregledi sistema (PQ) – analiza sistema;
- kontrola sprememb (Change Control in GAMP nivo 0, 1, 2, 3, 4).

Glede na obseg in zahtevnost projekta se lahko posamezni segmenti združujejo oziroma se jih ne izvaja. **Krovna mapa** mora vsebovati: kazalo, zahteve za sistem, opis sistema, opis platform, načrt infrastrukture v grafični obliki in opisno, ključne specifikacije sistema in zahteve za okolje, oceno tveganj z opisom ukrepov, zgodovino kontrole sprememb, podatke o izvedenih testiranjih, prehod na produkcijo, opis upravljanja konfiguracij, opis vlog na sistemu, upravljanje avtorizacij, evidenco napak in posegov, preventivno vzdrževanje, back-up/recovery postopke in periodično preverjanje, nadzor delovanja in spremljanje obremenjenosti, upravljanje varnosti (protivirusna zaščita, varnostne popravke itd.), izobraževanje, obvladovanje dobaviteljev, vzdrževalne pogodbe. V tem procesu nastajajo naslednji dokumenti:

Plan kvalifikacije (angl. *Validation Master Plan*, v nadaljevanju VMP). VMP mora definirati aktivnosti, postopke in odgovornosti za izvedbo posameznih aktivnosti v življenjskem ciklu sistema. Prav tako je v VMP definiran časovni načrt posameznih aktivnosti. V VMP se definira tudi način šifriranja dokumentacije, ki v življenjskem ciklu sistema nastaja. Odobren mora biti s strani vodstva podjetja, ki s svojim strinjanjem potrdi vire, potrebne pri izgradnji sistema.

Uporabniške zahteve (angl. *User Requirements Specification*, v nadaljevanju URS). Uporabniške zahteve so dokument, v katerem so postavljeni želeni cilji, ki jih mora sistem dosegati. Dokument pripravi uporabnika, lahko pa ga pripravi tudi dobavitelj. Dokument mora biti pregledan in odobren s strani odgovornega uporabnika in odgovorne osebe za kakovost.

Presoja dobavitelja. V primeru, da predstavlja računalniški sistem pretežni del sistema in je razvoj sistema delo zunanjih dobaviteljev je potrebno opraviti presojo dobavitelja. Dobavitelj mora uporabljati sistem kakovosti, ki zagotavlja kakovost, vgrajeno v sistem ter vso potrebno dokumentacijo. Certifikat o sistemu kakovosti (na primer ISO certifikat) ni zadosten dokaz, da je računalniški sistem kvalificiran in ne zagotavlja dovolj visoke stopnje dokumentacije, ki je potrebna s strani Krke, da ustreza vsem predpisom, omenjenim prej.

Funkcionalna specifikacija (angl. *Functional Specification*, v nadaljevanju FS). Funkcionalna specifikacija je dokument, ki ga pripravi izvajalec in s katerim odgovori na zapisane želje uporabnika, definirane v uporabniških zahtevah. Podpisana in odobrena (s strani uporabnika in dobavitelja) funkcionalna specifikacija je osnova za začetek izgradnje specifikacije dizajna. Funkcionalna specifikacija je hkrati tudi vodilo za pripravo funkcionalnega testiranja sistema.

Dizajn specifikacija (angl. *Design Specification*, v nadaljevanju DS). Dizajn specifikacija je dokument, pripravljen s strani dobavitelja, ki vsebuje natančen opis rešitve (strojne in programske opreme) in implementacijo sistema v obstoječe okolje. Prav tako so v dokumentu opredeljeni načini programiranja in vsi potrebni pogoji, potrebni za nemoteno delovanje v realnem obstoječem okolju. Dizajn specifikacija je vodilo za pripravo kvalifikacij namestitvev (IQ) in preverjanje pravilnosti dejansko vgrajenih komponent. Dizajn specifikacija mora biti pregledana in odobrena s strani odgovornih oseb na projektu.

Specifikacija strojne opreme (angl. *Hardware design specification*, v nadaljevanju HDS). Potrdi jo skrbnik sistema. Tehnični opis zajema:

- opis konfiguracije strojne opreme (strežnik, PC, stikalo, PLC, I/O moduli, komunikacijski moduli, regulatorji, pogoni, mreža, procesna mreža, ipd.),
- opis povezav z ostalimi sistemi,
- opis strojne opreme s tehničnimi specifikacijami.

Specifikacija programske opreme (angl. *Software design specification*, v nadaljevanju SDS). Specifikacija programske opreme, ki jo potrdi skrbnik sistema, zajema:

- podrobni opis načrta, arhitekturo, obseg, funkcije, programsko strukturo, diagrame poteka,
- podroben opis podatkovnih struktur,
- povezave med sistemi in opisi povezav,
- opis nastavitev in konfiguracij.

Kvalifikacija namestitve (angl. *Installation Qualification*, v nadaljevanju IQ). Postopek kvalifikacije namestitve mora biti pripravljen in pregledan pred izvedbo in odobren po sami izvedbi. Odobren in pregledan je s strani oseb, definiranih v VMP. S pomočjo IQ-ja preverimo (obseg aktivnosti je odvisen od samega sistema – poslovni ali procesni sistem):

- ustreznost vgrajene opreme,
- pravilnost vgradnje opreme,

- pravilnost prenosa signalov od periferne opreme do prikaza na nadzornem sistemu,
- potrebne pogoje za pravilno delovanje sistema,
- vhodno izhodne enote (potrebna je kalibracija merilnih instrumentov),
- testiranje analognih in digitalnih signalov (kalibracija merilnih zank),
- preverjanje potrebnih dokumentov za nemoteno delo in vzdrževanje sistema,
- testiranje ustreznosti vgrajene programske opreme:
 - sistemska programska oprema,
 - aplikativna programska oprema,
- testiranje varnosti in zaščite.

Na koncu izvedenih aktivnosti sledi zaključno poročilo testiranja sistema.

Kvalifikacija delovanja (*Operational Qualification*, v nadaljevanju OQ). OQ postopek mora biti pripravljen in pregledan pred izvedbo ter odobren po sami izvedbi. Odobren in pregledan je s strani oseb, definiranih v VMP. Pred izvedbo testiranj morajo biti pripravljeni standardni operativni postopki, ki so potrebni za nemoteno delo s sistemom.

V sklopu testiranj OQ računalniškega sistema se izvajajo naslednja testiranja:

- testiranje funkcionalnega delovanja sistemov,
- testiranje sistema na stresne situacije – delovanje v kritičnih situacijah,
- testiranje ustreznosti zapisov podatkov v arhiv (zgodovina),
- testiranje delovanja sledljivosti,
- testiranje ustreznosti sistema kontrole dostopov in zaščit sistema,
- testiranje poročil elektronskih zapisov ter elektronskih podpisov.

Na koncu izvedenih testiranj sledi zaključno poročilo funkcionalnega testiranja sistema.

Zaključno poročilo. Zaključno poročilo je del življenjskega cikla, ki ga pripravi odgovorni skrbnik skupaj z izvajalcem. Vanj se zapiše vse izvedene aktivnosti, ki dokazujejo pravilnosti delovanja sistema. Navede se tudi poročilo o izvedenem izobraževanju vzdrževalcev sistema. Zapišejo se pomanjkljivosti v sistemu in odstopi ter način in rok za odpravo le-teh. Zapisnik podpišeta predstavnik izvajalca in predstavnik naročnika ter osebe, definirane v VMP.

Ko je zaključno poročilo zaključeno, se sistem smatra v celoti operativen in teče v produkcijskem okolju podjetja. Skozi celoten življenjski cikel živega sistema se ob spremembah na sistemu, nadgradnjah ipd., nenehno vzdržuje vsa omenjena dokumentacija,

odvisno pač od segmentov, v katerih so izvajajo spremembe.

3.6 Ocena posledic vpeljave upravljanja identitet

Vodstvo sektorja ITT in tudi vodstvo podjetja je ugotovilo, da smo s povečanjem števila zaposlenih v zadnjem desetletju in čedalje strožjim nadzorom sledljivosti pravic zaposlenih in doslednem ukinjanju teh pravic prišli do situacije, ko so časovne dobe izvajanja sprememb na teh objektih predolge, sledljivost preslaba ter poročila netočna, pomanjkljiva ali pa ne obstajajo. Že vrsto let smo v Krki vpeljevali sisteme, ki so bili vse bolj integrirani med seboj, saj smo še inženirji opazali težave prav z administracijo uporabnikov neintegriranih sistemov. Odločitev o vpeljavi sistema identitet je izhajala tako s strani uprave, kot je bila dobrodošla s strani zaposlenih, ki so imeli največ administrativnega dela prav z upravljanjem identitet – oziroma posameznikov in njihovih dostopov do sistemov.

Sistem za upravljanje identitet igra danes zelo pomembno vlogo v sistemu, ki predvsem s stališča zagotavljanja ustreznosti s strogim predpisom in standardom, omogoča sledljivost vseh sprememb dostopov in drugih dogodkov, izdelavo poročil, potrebnih za presoje sistemov in skrbi za varnost dostopov – torej tudi pravočasno ukinjene dostope ob izstopu zaposlenega.

Odločitev o izbiri dobavitelja nam je predstavljala kar precejšen izziv. Kot sem opisal v nalogi, imamo na eni strani zelo močne vodilne igralce na področju IdM, na drugi strani pa imamo v Krki okolje, ki je zelo močno povezano z Microsoftovimi tehnologijami (kot so aktivni imenik, elektronska pošta, intranet storitve ipd.) in prav tako smo s podjetjem Microsoft dolgoletni partnerji ter tudi partnerji z nekaterimi podizvajalci podjetja Microsoft, ki že zelo dobro poznajo naše sisteme in postopke. Microsoft je s svojimi podizvajalci, ki so zelo dobro poznali sistem Omada, pripravil kvalitetno ponudbo, ki se je bila v prvi vrsti zelo dobro umeščena v integriran sistem Krke, po drugi strani pa smo dobavitelja zelo dobro poznali in nam je to predstavljalo tudi bistveno manjši odpor pri implementaciji takega sistema. Samih referenc v Sloveniji ni prav veliko, saj se, podobno kot smo mi izvajali vpeljavo sistema, tudi po drugih podjetjih uvaja večinoma fazno in po principu gradnje najprej nastavi temelje (torej povezavo kadrovske službe in imenika, upravljanje elektronske pošte), nato se dogradi sistem za upravljanje vstopov in izstopov, upravljanje vlog itn.

Za uspešno vpeljavo sistema pa je potrebno pripraviti tudi primerno okolje. Večino sistemov smo že imeli povezanih z aktivnim imenikom (sistem avtentikacij in avtorizacij poteka preko aktivnega imenika), zato je smiselno aktivni imenik uporabiti kot centralno skladišče javnih podatkov – torej podatkov, ki so lahko na voljo vsem uporabnikom. V aktivni imenik pa prečrpavamo podatke iz avtoritativnih virov, kadrovske baze in SAP HR-

ja. Po drugi strani pa je ključnega pomena tudi kvalitetna definicija procesov (na primer vstopa, izstopa in ostalih zahtev, opredeljenih v poglavju 3.2), saj le tako lahko dosežemo cilje celostno in učinkovito.

Včasih predstavljajo problem tudi posamezniki v projektni skupini, še posebno, če ne razumejo namena in ciljev projekta oziroma ne vidijo, kako bo to doprineslo dodatno vrednost podjetju. V primeru upravljanja identitet, ki je s strani sistemskih inženirjev nekako nejasen cilj, saj naj se vsega ne bi dalo upravljati z »enim gumbom«, lahko prav ti povzročijo največ težav pri projektu zato je pomembno, da vodja definira prvotne cilje jasno in karseda enostavno, z jasnimi cilji. Člane projektne ekipe je smiselno tudi stimulirati, saj je projekt vpeljave sistema za upravljanje identitet navadno dolgotrajen projekt z več fazami.

Kljub temu pa prav posebnih težav s projektno skupino in samim postopkom vpeljave sistema v Krki nismo imeli. Še največji problem je velikost projekta, ki je na nivoju celotne Krke, kar pa zahteva odločitve iz več sektorjev in služb in že sama koordinacija posameznikov je občasno zelo velik problem. Delegiranje odgovornosti se pokaže kot zelo dober vzvod pri doseganju tehničnih ciljev, vsebinska definicija procesov pa je ključnega pomena za doseg teh ciljev.

V projektu vpeljave sistema za upravljanje identitet smo v Krki zaključili celotno prvo fazo funkcionalne vpeljave sistema – torej je sistem realiziran in v uporabi, vendar trenutno izvaja le funkcionalnost, ki sem jo opisal v poglavju 3.2. Gre za upravljanje uporabnikov, upravljanje skupin, vstopa in izstopa. Nekaj problemov se je pokazalo pri vpeljavi postopka izstopa, saj le-tega sedaj nismo izvajali dosledno in ko je sistem onemogočil nekaj računov in dostopov oseb, ki niso več imeli potreb po teh resursih, je prišlo do občasnih pritožb uporabnikov, ki pa so na koncu le uvideli, da je sistemsko tako pravilno.

Sistem za upravljanje identitet je v Krki živ sistem, ki še raste in v pripravi so tudi že nadaljnje faze sistema, kot je vpeljava avtorizacij na sistemih prek upravljanja vlog ipd. Nekaj smernic za nadaljevanje projekta bom podal že v sklepu naloge.

Nenazadnje pa je za nas bila zelo pomembna tudi dokumentacija (kot sem že omenjal večkrat v nalogi), ki zahteva veliko dela, vendar brez dokumentacije v Krki ne moremo več vpeljati novega sistema. Še posebno v lanskem letu, ko smo se pripravljali na presojo ameriške FDA, je bilo in še vedno je, nujno potrebno urejati dokumentacijo v skladu z njihovimi predpisi in standardi.

Ključni faktorji uspeha. Upravljanje identitet se za marsikoga zdi torej projekt v »oblakih« in le s strpnim faznim pristopom lahko skozi dolgotrajne postopke realiziramo

celotno upravljanje identitet skozi en vmesnik. Idealno stanje je torej tako, da ko se oseba zaposli v Krki na določeno delovno mesto, avtomatsko pridobi vse pravice in dostope, ki jih omenjeno delovno mesto potrebuje, prejme uporabniško ime, naslov elektronske pošte, delegirane pravice v proizvodnih in poslovnih sistemih itd. Da bi to lahko dosegli učinkovito, menim, da so ključni faktorji uspeha naslednji:

- dobra analiza obstoječega stanja,
- priprava (faznega) načrta vpeljave,
- sestava dobre projektne ekipe,
- zagotovljena podpora vodstva,
- zagotovljena dodatna potrebna sredstva.

Posamezne postavke sem opredelil že v nalogi sami. Uporabniške zahteve predstavljajo analizo stanja in cilje projekta. V Krki je to najpomembnejši dokument za uspešno realizacijo projekta. Težko si predstavljamo uspešen projekt brez kvalitetne projektne skupine. Projektni vodja mora skupaj z vodstvom podjetja izbrati prave kadre in jim jasno opredeliti cilje in naloge, da je lahko ekipa uspešna. Podpora vodstva je nujna pri vseh projektih, ki se dotikajo tudi dela v drugih službah, saj lahko odpor uporabnikov omaja še tako dober projekt. Vodstvo v Krki se zaveda pomena upravljanj identitet in je sam projekt uvrstilo med vsebinsko pomembnejše projekte v zadnjih letih. Posledično je vodstvo nudilo izdatno podporo projektu ter zagotavljalo ostala potrebna sredstva projektni ekipi (kadre iz drugih služb, svetovalce ipd.)

Poslovna vrednost vpeljanega IdM sistema. Prednosti in slabosti vpeljave IdM sistema v podjetje sem opredelil s stališča literature že v uvodnem delu naloge. Če na kratko povzamem bistvo, je vpeljava takega sistema predvsem finančno veliko breme ter tudi zelo zahtevna naloga, kar pa je pogojeno tudi z okoljem podjetja, kjer vpeljujemo tak sistem. Prednosti pa ležijo v posledično večji obvladljivosti nadzora nad uporabniškimi dostopi, pravicami ter avtomatizacijo delegiranja teh pravic na ustrezne sisteme v podjetju.

Samo poslovno vrednost v smislu ustvarjanja direktnega prihodka in dobička bi zelo težko predstavili brez uporabe dejanskih stroškov in kompleksnih meritev izvajanja posameznih operacij. Skozi proces opazovanja in uporabe sistema v podjetju sem ugotovil, da se še vedno največ časa izgubi s čakanjem na odobritev pred izvedbo naslednjega koraka v procesu. Prav tako je bil v začetku prisoten odpor do uporabe novega orodja in kot sem opazil, je bil izvor predvsem v nedosledni urejenosti posameznih okolij. Te nedoslednosti smo v veliki meri uspešno odpravili, vzpostavili sledljivost spremembam in jasen pregled nad obstoječim stanjem. Ker smo se prehoda lotili »mehko«, torej smo na posameznih sistemih omogočali prehodno obdobje, kjer smo še dopuščali ročno urejanje dostopov, je bil sam proces bistveno manj stresen in je skrbnikom omogočil dovolj časa za ureditev

stanja. Dosledna uporaba sistema upravljanja identitet torej prinaša veliko mero urejenosti in preglednosti uporabniških dostopov na raznih podsistemih in tudi ponuja vmesnik za enovit nadzor nad različnimi podsistemi, kar je ena izmed njegovih ključnih vrednot.

V poglavju 3.2 sem predstavil uporabniške zahteve, ki so temelj vzpostavitve projekta v Krki in hkrati odražajo končno funkcionalnost, ki jo želimo z vpeljavo IdM sistema doseči. V okviru uporabniških zahtev sem med drugim predstavil tudi nekaj procesov upravljanja uporabniških in računalniških računov ter upravljanja s skupinami. To so samo osnovni procesi, ki so bili modelirani posebej za potrebe projekta. Skozi nadaljnje faze projekta, ki še sledijo v prihodnjih letih, nekateri pa se že izvajajo, smo in bomo modelirali tudi ostale procese v podjetju, kjer lahko kaj pridobimo z vpeljavo takega sistema. Sistem upravljanja identitet kot računalniški sistem nam poleg nadzorne plošče za nastavljanje pravic omogoča tudi izvajanje teh procesov, bodisi samostojno ali preko ostalih podsistemov. Avtomatizacija omogoča hkrati hitrejšo in pravilnejšo izvajanje posameznih korakov v procesu kot pa ročno delo, ki je podrejeno človeškim napakam. Hitrost in natančnost izvajanja procesov sodi med poslovno vrednost takega sistema, kot tudi prej omenjena urejenost, preglednost in sledljivost posameznih identitet. Na žalost pa možnost človeške napake lahko poslovno vrednost avtomatskega procesa spremeni tudi v poslovno škodo, saj faktor človeške napake ostaja v načrtovanju procesa. Kot primer lahko povem, da smo v projektu preveč ohlapno definirali proces odstranjevanja računalniških računov iz aktivnega imenika. Zaradi tega je ob nepravilni definiciji nabora računalnikov za odstranitev prišlo do človeške napake, ki je povzročila odstranitev prevelikega števila osebnih računalnikov iz sistema. Posledično te naprave niso več imele dostopa omrežja in virov, s tem pa je nastala poslovna škoda. Kljub temu, da je bil vzrok človeški faktor, je možnost takega opravlila prinesel sistem IdM v svojem internem procesu, ki je bil definiran tekom projekta in brez IdM sistema ni bil možen.

Če izvajamo posamezne napake, ki se pri gradnji tako kompleksnih sistemov lahko zgodijo, lahko z trdimo, da je avtomatizacija in računalniška obdelava točna, hitra in z dobro definiranimi procesi razbremenjuje ljudi, ki so opravljali te procese. V primeru službe informatike v Krki smo to predvsem skrbniki sistemov, v pogledu podjetja kot celega pa tudi vse uporabniki, ki upravljajo kakršnekoli dostope do virov v podjetju. Ker smo farmacevtsko podjetje, ki izdeluje zdravila, smo nenehno presojeni s strani raznih inštitucij, ki iz leta v leto višajo standarde, katerim smo podvrženi. Naloga vsakega skrbnika sistema in vseh, ki upravljajo dostope do posameznih virov, je vzdrževanje ažurnega stanja dostopov in sledljivost spremembam v dostopih skozi čas. Z uporabo orodij, ki jih je vpeljal sistem upravljanja identitet, smo razbremenili te vire, ki se lahko več časa posvečajo ostalim nalogam. Sistem upravljanja identitet je v okviru mojega delovnega mesta kot skrbnika sistemov in upravljavca dostopov povečal storilnost in mi omogočil več časa za opravljanje tekočega dela.

SKLEP

Posledice dostopov uporabnikov, ki nimajo pooblastil dostopa do informacijskih in drugih virov v podjetju, so lahko tudi usodne za podjetje, zato je nujno potrebno poskrbeti za uporabo sistema, ki zagotavlja varnost, sledljivost in možnost izdelave poročil o dostopih uporabnikov. Prav tako pa mora sistem delovati po vnaprej pripravljenih postopkih in procesih, ki definirajo vloge in uporabniške dostope. Najpomembnejša vidika pri odločitvi in vpeljavi sistema za upravljanje identitet vidim v **avtomatizaciji procesov** – torej povezavo sistemov med seboj do te mere, da se enotna identiteta uporabnika uporablja skozi vse povezane sisteme in po drugi strani sistem omogoča **upravljanje in sledljivost identitete**.

Avtomatizacija procesov ali avtomatsko dodajanje dostopov zaposlenim na sisteme uredi in olajša ter pohitri samo kreiranje nove identitete v podjetju ter poskrbi za to, da ta zaposleni dejansko pridobi vse potrebne pravice na sistemih, ki jih uporablja pri svojem dnevnem delu. Taka izvedba v prvi vrsti zelo strogo spoštuje vnaprej definiran proces in izloči človeški faktor kot možnost napake pri dodeljevanju dostopov. Sistem tudi sam poskrbi, da pravočasno odstrani pravice, ki jih zaposleni ne potrebuje več.

Z avtomatizacijo procesov prihranimo veliko časa in denarja pri uvajanju novih zaposlenih, premestitvah na druga delovna mesta, saj bistveno zmanjšujemo količino dela, ki ga sedaj porabimo za ročno izvedbo procesov. Z vpeljavo sistema IdM si tudi na enem mestu zagotovimo nadzorovanje in beleženje vseh sprememb, povezanih z upravljanjem identitet za vse povezane sisteme, s čimer smo tudi skladni z zakonodajo, predpisi, standardi in dobro prakso.

V sami nalogi sem opisal samo nekaj procesov, ki smo jih spreminjali neposredno, hkrati pa so se spremenili še ostali procesi, ki se nanašajo na te osnovne procese. Kot sem omenil, je ključna prednost sledljivost in samo dejstvo, da se proces izvaja točno tako »kot bi se moral« skozi avtomatiziran nabor pravil izvajanja procesa. Avtomatizirano izvajanje pa ni zgolj prednost, saj nas do neke mere omejuje s tem, kar predpišemo, kdaj in kako naj bi se zgodilo (program, postopek). Ker smo prenos podatkov med sistemi zasnovali kot sinhronizacijski proces, je to obdobje čakanja na sinhronizacijo tako slabost kot tudi prednost vpeljanega sistema. Slabost se izraža kot zmanjšana agilnost podjetja pri izvedbi določenih nalog (na primer kreiranje poštnega nabiralnika vzame skrbniku sistema zgolj nekaj minut za izvedbo, medtem ko se sinhronizacija izvaja vsaki dve uri in pomeni čakanje na izvedbo daljši čas, kot brez uvedbe sistema). V večini primerov nam to ne povzroča težav, če pa je nujno, pa sistem omogoča ročni zagon sinhronizacije. Prednost sinhronizacije po urniku pa se kaže v tem, da so podatki pripravljeni bolj strukturirano, uporabljamo enotni vmesnik za izvedbo in omogoča pregled pred izvedbo ter tudi

sledljivost izvedbi samih opravil. Glede na stroge regulative, v katerih deluje farmacevtsko podjetje, je slednje ključnega pomena za uspešno zagotavljanje kvalificiranega delovnega okolja.

Upravljanje in sledljivost identitet skozi njihov celoten življenjski cikel je ključna funkcionalnost orodja upravljanja identitet. Življenjski cikel identitet definiramo s politiko v podjetju, medtem ko nam vpeljana orodje omogoča enostavno prilagajanje življenjskih ciklov našim potrebam.

Izziva na projektu, ki sta mi osebno predstavljala najbolj zanimivo področje, sta bila zagotovo priprava procesov upravljanja skupin in računalniških objektov ter pristop k analizi ponudb in sam izbor ponudnika. V okviru projekta sem večinoma zastopal naloge sistemskih skrbnikov in naše vloge kot upravljavcev vsebin. Definiral sem procese predvsem za področje upravljanja skupin in računalniških objektov, sodeloval pri tehnični implementaciji v testnem in kasneje produkcijskem okolju. Izziv definiranja procesov in dokumentiranja postopkov, ki jih opravljamo v našem oddelku, se sprva zdi suhoparen. Vendar je meni kot sistemskemu skrbniku omogočil vpogled v skupni proces upravljanja identitet in tudi bolje razumeti vlogo in pomen dobre urejenosti in preglednosti predvsem osnovnih infrastrukturnih storitev kot temelja gradnje celostne rešitve upravljanja identitet. Poleg tega sem imel možnost avtomatizacije izvajanj posameznih, posebej perečih dolgotrajnih procesov, kjer ni manjkalo tehničnih izzivov.

Ker je projekt sistema upravljanja identitet v prvotnih fazah predvideval integracijo osnovnih infrastrukturnih storitev ter kadrovskega sistema, smo skupino za izbor ponudnika sestavili znotraj službe IT. Visoki stroški projekta, v katere smo všteli tudi stroške potrebnih sprememb v infrastrukturi podjetja, so nas silili v zelo natančno in kompleksno pripravo uporabniških zahtev, iz katerih smo nato pripravili razpisno dokumentacijo. Ponudb sicer ni bilo veliko, kar tudi ni pričakovati, saj potrebe podjetja presegajo sposobnosti večine manjših ponudnikov rešitev na trgu. Izbirali smo med štirimi ponudbami, ki so ustrezale razpisni dokumentaciji. Sistem kriterijev in uteži smo dalj časa usklajevali in večkrat spreminjali, preden smo uskladili vse poglede posameznikov, vključenih skupino. Kot sem predstavil tudi v primeru v točki 2.3.3.1, smo najpomembnejši kriterij za izbiro ponudnika še dodatno razčlenili v podsistem kriterijev in uteži, da bi tako dobili čim bolj realno oceno ustreznosti rešitve glede na razpisno dokumentacijo oziroma uporabniške zahteve. Ocenjevanje ponudnikov in posameznih kriterijev je bila najbolj zahtevna naloga skupine, saj smo morali ob dolgotrajnem pregledovanju ponudb upoštevati še vse potrebne notranje posege, ki bi jih določena rešitev prinesla. Kot sem omenil v uvodu naloge, je vpeljava IdM sistema zelo povezana z obstoječimi infrastrukturnimi storitvami, ki jih že uporabljamo v podjetju, zato smo morali skrbno pretehtati prav ta segment ponudb, saj bi nam slaba izbira lahko kasneje prinesla visoke dodatne stroške. Menim, da smo analizo in izbor opravili kakovostno in pošteno, upoštevajoč tako dobavitelje, ponudbe kot tudi najbolj optimalno rešitev za samo podjetje.

V magistrskem delu sem skušal celostno predstaviti, kako se v večjem podjetju lotiti vpeljave sistema upravljanja identitet ter kaj so najpomembnejši cilji projekta, ki jih želimo doseči. Kot smo spoznali, je vpeljava takega sistema izredno dolgotrajna in nujno razdeljena v faze. Kot menijo nekateri skeptiki, se vseh sistemov ne da povezati – vendar smo skozi nalogo spoznali, da je to možno ob strpnem in skrbno načrtovanem faznem pristopu k realizaciji projekta.

Upravljanje identitet prinaša precej prednosti, sledljivosti in možnosti poročanja, ki jih pred uvedbo sistema nismo imeli. Glede na čedalje strožje predpise in standarde na področju farmacije je vpeljava sistema upravljanja identitet za Krko nujna in hkrati tudi zelo dobrodošla. Rezultati uporabe sistema so danes vidni predvsem v hitrejšem, bolj točnem, urejenem in preglednem nadzoru in upravljanju dostopov do velikega števila elektronskih virov v podjetju. Projekt uvajanja sistema upravljanja še ni zaključen in ostaja kontinuirani proces vpeljave že obstoječih in tudi novih sistemov v podjetje, pod okrilje nadzora z uporabo sistema za upravljanje identitet.

LITERATURA IN VIRI

1. Ahuja, J. (2004). *Identity Management: A Business Strategy for Collaborative Commerce*. Najdeno 5.4.2012 na spletnem naslovu <http://www.isaca.org/Journal/Past-Issues/2003/Volume-6/Documents/jpdf036-IdentityManagement-BusinessStrategy.pdf>
2. Bergman, M. & Cooper, J. (2006) *Identity Management for the Rest of Us: How to Grow a New Infrastructure*, Educause Mid-Atlantic Regional Conference. Baltimore, ZDA
3. Bisaerts, D. (2011). *Top 5 Identity Management vendors of today*. Najdeno 11.3.2012 na spletnem naslovu <http://www.itsecurity.be/top-5-identity-management-vendors-of-today>
4. Bokal, M. (2008). *Vzpostavitev enotnega Aktivnega imenika na Univerzi v Ljubljani*. Najdeno 5.4.2012 na spletnem naslovu <http://dkum.uni-mb.si/IzpisGradiva.php?id=9461>
5. Bowie, A. (1993). *Schelling and modern European philosophy*. (str. 55-90). Routledge.
6. Burton Group (2009). *Provisioning Market 2009: Divide and Conquer*. Najdeno 15.4.2012 na spletnem naslovu <http://www.oracle.com/us/products/middleware/identity-management/059366.pdf>
7. Burton Group. (2005). *Oracle's Approach to Identity Management*. Burton Group.
8. Camp, J.L. (2004). *Digital Identity* (št. 3, zv. 23). IEEE Technology and Society Magazine.
9. Ciglarič, M., Krevl, A. & Pančur, M. (2008). *Strategija upravljanja z digitalnimi identitetami na Univerzi v Ljubljani*. (v1.0). Univerza v Ljubljani.
10. De Clercq J. & Rouault, J. (2009). *An Introduction to Identity Management*. Najdeno 8.11.2011 na spletnem naslovu http://iranmath.googlepages.com/idmgt_intro.pdf
11. Ferraiolo, D. & Kuhn, R.(2004). *Role Based Access Control, American National Standard for Information Technology*. NIST.
12. Ferraiolo, D., Kuhn, R. & Sandu, R.(2000). *The NIST Model for Role-Based Access Control: Towards A Unified Standard*. NIST.
13. Food and Drug Administration. (2003). *Guidance for Industry, Part 11, Electronic Records*. Najdeno 3.2.2012 na spletnem naslovu <http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm>
14. Gartner Research. (2008). *Magic Quadrant for User Provisioning*, Najdeno 3.2.2012 na spletnem naslovu <http://www.identropy.com/blog/?Tag=Gartner%27s%20Magic%20Quadrant>
15. HP. (2009). *The HP Security Handbook*. Najdeno 5.4.2012 na spletnem naslovu <http://h71028.www7.hp.com/ERC/downloads/HP%20Security%20Handbook%20V2.pdf>
16. Hunter, L. & Allen, R. (2008). *Active Directory Cookbook, 3rd Edition*. O'Reilly Media

17. ISACA. (2008). *IT Governance Institute: CobiT*. Najdeno 8.9.2011 na spletnem naslovu <https://www.isaca.org/Pages/default.aspx>
18. ISPE. (2012). *GAMP: Good Practice Guides*. Najdeno 16.5.2012 na spletnem naslovu <http://www.ispe.org/gamp-good-practice-guides>
19. Jagannathan, S. (2009). *Social Network and Identity Management SIM*. Tata Elxsi Limited. Najdeno 9.9.2011 na spletnem naslovu http://www.iimahd.ernet.in/sim09/Speakers/S_Jagannathan.pdf in <http://www.iimahd.ernet.in/sim09/>
20. Kaufman, K. (2003). *GIAC Security Essentials Certification (GSEC) Practical Assignment*. SANS Institute.
21. Košiček, M. (2004). *Informatizacija upravljanja kakovosti v podjetju Krka*. Magistrsko delo (str. 16-19). Univerza v Ljubljani, Ekonomska fakulteta.
22. Lukawiecki, R. (2012). *Project Botticelli, Business Intelligence*. Najdeno 5.4.2012 na spletnem naslovu <http://projectbotticelli.com/video>
23. Mann, B. (2009). *Computer Associates International: Seven Habits of high effective identity management*. Najdeno 17.3.2012 na spletnem naslovu http://www.computerworld.com/s/article/95200/Seven_habits_of_highly_effective_identity_management?taxonomyId=17&pageNumber=2
24. Marand. (2009). *Rešitve za celovito upravljanje identitet uporabnikov*. Najdeno 5.4.2012 na spletnem naslovu <http://www.marand.si/resitve/upravljanje-identitet/>
25. McQuaide, B. (2003). *Identity and Access Management*. Najdeno 8.9.2011 na spletnem naslovu <http://www.isaca.org/Journal/Past-Issues/2003/Volume-4/Pages/Identity-and-Access-Management.aspx>
26. META Group. (2002). *The Value of Identity Management: How securing identity management provides value to the enterprise*. META Group.
27. Microsoft. (2009). *Active Directory Architecture*. Microsoft Technet. Najdeno 9.9.2012 na spletnem naslovu <http://technet.microsoft.com/en-us/library/bb727030.aspx>
28. Microsoft. (2009). *Microsoft Identity Lifecycle Manager 2007 FP1*. Microsoft Technet. Najdeno 9.9.2012 na spletnem naslovu <http://www.microsoft.com/en-us/server-cloud/forefront/identity-manager.aspx>
29. Microsoft. (2010). *Forefront Identity Management 2010 Technical Overview*. Najdeno 9.9.2011 na spletnem naslovu [http://technet.microsoft.com/en-us/library/ff621362\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff621362(WS.10).aspx)
30. MNL Limited. (2012). Najdeno 16.5.2012 na spletnem naslovu <http://www.mnl-limited.com/services.htm>
31. Moj Mikro. (2009). *Upravljanje digitalnih identitet*. Najdeno 5.9.2009 na spletnem naslovu http://www.mojmikro.si/mreza/uporabno/upravljanje_digitalnih_identitet
32. Office of Government Commerce. (2007). *ITIL Service Operation*. The Stationery Office
33. Oracle. (2009). *Oracle Identity Manager Documentation*. Oracle Corp. Najdeno

16.5.2012 na spletnem naslovu

http://download.oracle.com/docs/cd/E10391_01/index.htm

34. Oracle. (2010). *Oracle Identity Management*. Oracle Corp. Najdeno 16.5.2012 na spletnem naslovu <http://www.oracle.com/us/products/middleware/identity-management/index.htm>
35. Pfitzmann, A. & Hansen, M. (2010). *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management : A Consolidated Proposal for Terminology* (v0.34). Najdeno 5.4.2012 na spletnem naslovu http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf
36. Praprotnik, M. (2008). *Ena identiteta za enega uporabnika*. Finance št. 90, str. 32, Najdeno 9.9.2011 na spletnem naslovu http://www.simt.si/pdf/ena_identiteta_za_enega_uporabnika.pdf
37. Provost.(2004). *Identity Management Roadmap*. University of Toronto. Najdeno 5.4.2012 na spletnem naslovu <http://www.provost.utoronto.ca/public/reports/overview/appendices/a.htm>
38. Reed, A. (2002). *The Definitive Guide To Identity Management*. Realtime Publishers.
39. Rouse, M. (2007). *Authentication Definitions*. Najdeno 15.4.2012 na spletnem naslovu <http://searchsecurity.techtarget.com/definition/authentication>
40. Slovar infomatike. (2012). *Slovar informatike, II. izdaja*. Najdeno 5.4.2012 na spletnem naslovu <http://www.islovar.org>
41. Syngress. (2003). *Creating Security Policies And Implementing Identity Management With Active Directory*. Syngress.
42. Tracy, K. (2008). *Identity Management Systems* (št. 6, zv. 27, str. 34-37). IEEE Potentials.
43. Windley, P.J. (2005). *Digital identity*. (20 poglavij). O'Reilly Media.
44. Zveza potrošnikov Slovenije (2007). *Lažno predstavljanje ali »phishing«*. Najdeno 5.4.2012 na spletnem naslovu <http://www.zps.si/tehnologija/internet/lazno-predstavljanje-ali-phishing.html?Itemid=628>

PRILOGE

KAZALO PRILOG

Priloga 1: Slovarček uporabljenih kratic3-1

Priloga 2: Specifikacija sinhronizacije KIS-AD3-2

Priloga 1: Slovarček uporabljenih kratic

CRM	Customer relationship management (Sistem za upravljanje odnosov s strankami)
Courion	podjetje Courion
DNS	Domain Name System (sistem domenskih imen). Sistem za pretvarjanje IP naslova v spletnem naslovu. Za pretvarjanje skrbijo DNS strežniki.
ERP	Enterprise resource planning (celovite programske rešitve)
Exchange	Microsoft Exchange 2007 – sistem za elektronsko pošto
IBM	podjetje IBM
IdM	Identity Management (upravljanje z identitetami)
ILM	Identity Lifecycle Manager (programski paket podjetja Microsoft za upravljanje z identitetami).
IT	Information technology (informacijska tehnologija)
ITIL	Information Technology Infrastructure Library
ITT	Sektor za informacijske tehnologije in telekomunikacije v podjetju Krka.
Krka	podjetje Krka, d. d., Novo mesto
LDAP	Lightweight Directory Access Protocol
Microsoft	podjetje Microsoft Corporation
MIIS	Microsoft Identity Integration Server 2003 (rešitev za upravljanje z identitetami podjetja Microsoft)
Novell	podjetje Novell
OIM	Omada Identity Manager (rešitev za upravljanje z identitetami podjetja Omaga A/S)
Omada	podjetje Omada A/S (od leta 2012 v 100 % lasti podjetja Microsoft)
Oracle	podjetje Oracle
PKI	Public Key Infrastructure (infrastruktura javnih ključev)
SAP	Podjetje SAP
SAP ERP	Celovita programska rešitev podjetja SAP
SAP GRC	SAP Governance, Risk and Compliance (rešitev podjetja SAP za nadzor vodenja podjetja, tveganja in usklajenosti)
SCOM	Microsoft Service Center Operations Manager 2007 (program, ki ga v podjetju uporabljamo za nadzor delovanja sistemov in spremljanje napak na sistemih)

Priloga 2: Specifikacija sinhronizacije KIS-AD

POLJE V AD	HR	EX	AL	Ser	Ost	POLJE V HR	PRIMER	PRAVILO
Full Name	1	1	1	1	1		Kristan (01-00937)	
First Name	1	1					Matevž	
Last Name	1	1					Kristan	
Company	1	1				sifra_podjetja_org, naziv_podjetja	01 - Krka, d. d.	sifra_podjetja_org + '-' + naziv_podjetja
	1	1	1	1	1	idm_id	00000937	idm_id
User Logon Name User Logon Name (pre Windows 2000)	1	1	1	1	1	priimek, ime	kristanm	algoritem: - priimek - če že obstaja - priimek + prva črka imena ... - Zamenjava posebnih znakov
UPN	1	1	1	1	1		@corp.krka.biz	konstanta
Description	1	1	1	1	1	sifra_podjetja, maticsna	01-0937	sifra_podjetja + '-' + maticna
Department	1					sifra_oe, dolgi_naziv_oe	109942 - ODDELEK ZA SIST. PODPORO	sifra_oe + '-' + dolgi_naziv_oe
Title	1					sifra_dela, naziv_dela	0004 - INFORMATIK	sifra_dela + '-' + naziv_dela
Telephone number	1	1				telefon_stacionarni	7116	telefon_stacionarni
Mobile	1					telefon_mobilni	041720721	telefon_mobilni
Fax	1					fax	073317116	fax
Office	1					lokacija_delovnega_mesta	NOVO MESTO	naziv_lokacija_dm
Manager - Name	1	1				vodja	idm_id_vodje	vodja
Account expires	1	1	1	1	1		Never	Konstanta
User must change password at next logon	1	1						
Control access through Remote Access Policy	1	1	1	1	1			
Logon Workstations - The following computers			1					
User cannot change password			1	1				
Password never expires			1	1				
Display Name	1	1	1	1	1		Kristan, Matevž	
E-mail	1						matevz.kristan@krka.biz	
Alternative E-mail	1						matevz.kristan@terme-krka.si	
POLJE V KIS	TIP	POLJE V AD	SKUPINE ZAPOSLENIH					
SKUPINE ZAPOSLENIH			Krka, d.d. - redno zaposleni					
VNAŠALEC PODATKOV			KS - Slovenija					
			Krka Terme, Golf Oločec – redno zaposleni					
			Podjetja in predstavništva v tujini – redno zaposleni					
			Zaposleni preko agencij					
			Študenti					
sifra_podjetja	char(2)		01	02, 05	21-50 (podjetja), 51 (predstavništva)	11	11	
			KIS	KIS	SAP	KIS	KIS	
			SIFRA_PODJETJA	SIFRA_PODJETJA	case substring(PA0000-PERNR, 1, 3) 021 - 21 022 - 22 ... 050 - 50 001 - 51 052 - 52 ... 089 - 89	SIFRA_PODJETJA	SIFRA_PODJETJA	
sifra_podjetja_org	char(2)	Company	01	02, 05	21-50 (podjetja), 51 (predstavništva)	01	01	
			KIS	KIS	SAP	KIS	KIS	
			SIFRA_PODJETJA_ORG	SIFRA_PODJETJA_ORG	case substring(PA0000-PERNR, 1, 3) 021 - 21 022 - 22 ... 050 - 50 001 - 51 052 - 52 ... 089 - 89	SIFRA_PODJETJA_ORG	SIFRA_PODJETJA_ORG	
naziv_podjetja	varchar(40)	Company	Krka, d. d.	Terme Krka	Krka Poljska	Krka, d. d.	Krka, d. d.	
			KIS	KIS	SAP	KIS	KIS	
			NAZIV_PODJETJA	NAZIV_PODJETJA	PA0001-BUKRS c(4) T001-BUKRS c(4) T001-BUTXT c(25) T001-SPRAS	NAZIV_PODJETJA	NAZIV_PODJETJA	
kadrovsko_podrocje	varchar(4)		1000	1010	6000	1000	1000	
			KIS	KIS	SAP	KIS	KIS	
			KADROVSKO_PODROCJE	KADROVSKO_PODROCJE	PA0001-WERKS c(4)	KADROVSKO_PODROCJE	KADROVSKO_PODROCJE	
maticna	char(5)		7294	0001	12345	12345	23456	
			KIS	KIS	SAP-HR	KIS	KIS	
			MATICNA	MATICNA	substring(PA0000-PERNR, 4, 5)	MATICNA	MATICNA	
idm_id	varchar(8)		00007294	00000001	02112345	00212345	00223456	
			KIS	KIS	SAP-HR	KIS	KIS	
					CENTRAL PERSON			
					HRP1001-SOBID PA0000-PERNR = HRP1001-OBJID HRP1001-SCLAS = 'CP' ili CALL FUNCTION 'HR_CENTRALPERSON_GET_NUMBERS'			
			MATICNA	MATICNA		MATICNA	MATICNA	
priimek	varchar(40)		OBLAK	OBLAK	OBLAK	OBLAK	OBLAK	
			KIS	KIS	SAP-HR	KIS	KIS	
			IME	IME	P0002-NACHN c(40)	IME	IME	
ime	varchar(40)		MARKO	MARKO	MARKO	MARKO	MARKO	
			KIS	KIS	SAP-HR	KIS	KIS	
			PRIMEK	PRIMEK	P0002-VORNA c(40)	PRIMEK	PRIMEK	
sifra_oe	char(6)	Department	109926	109926	109926	109926	109926	
			KIS	KIS	SAP-HR	KIS	KIS	
			SIFRA_OE	SIFRA_OE	P0001-PLANS n(8) HRP1001-OBJID n(8) HRP1001-SOBID n(8) HRP1001-BEGDA dat HRP1001-ENDDA dat HRP1001-SUBTY c(4) = 'A003'	SIFRA_OE	SIFRA_OE	

dolgi_naziv_oe	varchar(80)	Department	ODDELEK ZA RAZVOJ KIS DOLGI_NAZIV_OE	ODDELEK ZA RAZVOJ KIS DOLGI_NAZIV_OE	ODDELEK ZA RAZVOJ SAP-HR P0001-PLANS n(8) HRP1001-OBUID n(8) HRP1001-SOBID n(8) HRP1001-BEGDA dat HRP1001-ENDDA dat HRP1001-SUBTY c(4) = 'A003' HRP1000-OBUID n(8) HRP1000-STEXT c(40) HRP1001-BEGDA dat HRP1001-ENDDA dat	ODDELEK ZA RAZVOJ KIS DOLGI_NAZIV_OE	ODDELEK ZA RAZVOJ KIS DOLGI_NAZIV_OE
sifra_oe_nivo	char(6)		109926 KIS SIFRA_OE_NIVO	109926 KIS SIFRA_OE_NIVO	109926 SAP-HR P0001-PLANS n(8) HRP1001-OBUID n(8) HRP1001-SOBID n(8) HRP1001-BEGDA dat HRP1001-ENDDA dat HRP1001-SUBTY c(4) = 'A003'	109926 KIS SIFRA_OE_NIVO	109926 KIS SIFRA_OE_NIVO
sifra_dela	char(4)	Title	1056 KIS SIFRA_DELA	1056 KIS SIFRA_DELA	1056 SAP-HR P0001-PLANS n(8) HRP1000-OBUID n(8) HRP1000-SHORT c(12) HRP1000-BEGDA dat HRP1000-ENDDA dat	1056 KIS SIFRA_DELA	1056 KIS SIFRA_DELA
naziv_dela	varchar(45)	Title	VODJA PODROČJA KIS NAZIV_DELA	VODJA PODROČJA KIS NAZIV_DELA	VODJA PODROČJA SAP-HR P0001-PLANS n(8) HRP1000-OBUID n(8) HRP1000-STEXT c(40) HRP1000-BEGDA dat HRP1000-ENDDA dat	VODJA PODROČJA KIS NAZIV_DELA	VODJA PODROČJA KIS NAZIV_DELA
status	varchar(1)		3 KIS STATUS	3 KIS STATUS	3 SAP-HR P0000-STAT2	3 KIS STATUS	0 KIS STATUS
datum_vstopa	datetime		14.10.1996 KIS DATUM_VSTOPA	14.10.1996 KIS DATUM_VSTOPA	14.10.1996 SAP-HR CALL_FUNCTION 'HR_ENTRY_DATE'	14.10.1996 KIS DATUM_VSTOPA	14.10.1996 KIS DATUM_VSTOPA
datum_zaključka	datetime		31.12.2008 KIS DATUM_ZAKLJUČKA	31.12.2008 KIS DATUM_ZAKLJUČKA	31.12.2008 SAP-HR PA0000-ENDDA dat zadnji, kjer je PA0000-STAT2 = '3'	31.12.2008 KIS DATUM_ZAKLJUČKA	31.12.2008 KIS DATUM_ZAKLJUČKA
telefon_stacionarni	varchar(255)	Telephone number	2764 KIS TEL_INTERNA	2764 KIS TEL_INTERNA	2764 SAP-HR PA0105-USRID c(30) PA0105-SUBTY = 'INT'	2764 KIS TEL_INTERNA	2764 KIS TEL_INTERNA
telefon_mobilni	varchar(255)	Mobile	051350925 KIS TEL_GSM	051350925 KIS TEL_GSM	051350925 SAP-HR PA0105-USRID c(30) PA0105-SUBTY = 'MOBI'	051350925 KIS TEL_GSM	051350925 KIS TEL_GSM
fax	varchar(255)	Fax	073312002 KIS TEL_FAX	073312002 KIS TEL_FAX	073312002 SAP-HR PA0105-USRID c(30) PA0105-SUBTY = 'FAX'	073312002 KIS TEL_FAX	073312002 KIS TEL_FAX
sifra_lokacija_dm	varchar(9)		NOVO MESTO KIS LOKACIJA_DM	NOVO MESTO KIS LOKACIJA_DM	JASTREBARSKO SAP-HR Preveri Tabela Lokacija (2. list v excelu) PA0001-WERKS = Tabela Lokacija.WERKS PA0001.BTRTL = Tabela Lokacija.BTRTL Tabela.Lokacija.WERKS_LOKACIJA = true Tabela.Lokacija.WERKS + '0000' Tabela.Lokacija.WERKS_LOKACIJA = false Tabela.Lokacija.WERKS + Tabela.Lokacija.BTRTL	NOVO MESTO KIS LOKACIJA_DM	NOVO MESTO KIS LOKACIJA_DM
naziv_lokacija_dm	varchar(80)	Office	NOVO MESTO KIS LOKACIJA_DM	NOVO MESTO KIS LOKACIJA_DM	JASTREBARSKO SAP-HR Preveri Tabela Lokacija (2. list v excelu) PA0001-WERKS = Tabela Lokacija.WERKS PA0001.BTRTL = Tabela Lokacija.BTRTL Tabela.Lokacija.WERKS_LOKACIJA = true T500P-NAME1 c(30) PA0001-WERKS = T500P-PERSA Tabela.Lokacija.WERKS_LOKACIJA = false T001P-BTEXT c(15) PA0001-WERKS = T001P-WERKS, PA0001.BTRTL = T001P-BTRTL	NOVO MESTO KIS LOKACIJA_DM	NOVO MESTO KIS LOKACIJA_DM
vodja	varchar(16)	Manager	kristanm KIS VODJA	kristanm KIS VODJA	kristanm KIS CENTRAL PERSON Sistemizirano mesto osebe P0001-PLANS n(8) HRP1001-OBUID n(8) Organizacijska enota osebe HRP1001-SOBID n(8) HRP1001-BEGDA dat HRP1001-ENDDA dat HRP1001-SUBTY c(4) = 'A003' Če obstaja relacija tipa A290 za organizacijsko enoto in neko sistemizirano mesto, je oseba na tem sistemiziranem mestu vodja. Če ta relacija ne obstaja, poščemo nadrejeno organizacijsko enoto in ponovno postopek.	kristanm KIS VODJA	kristanm KIS VODJA
username	varchar(16)		kristanm KIS USERNAME	kristanm KIS USERNAME	kristanm KIS PA0105-USRID c(30) PA0105-SUBTY = '0001'	kristanm KIS USERNAME	kristanm KIS USERNAME
mail	varchar(128)		kristanm KIS MAIL	kristanm KIS MAIL	kristanm KIS PA0105-USRID c(30) PA0105-SUBTY = '0010'	kristanm KIS MAIL	kristanm KIS MAIL