Univerza v Ljubljani

FRI Fakulteta za računalništvo in informatiko

Siniša Jojić

Upravljanje identitet s pomočjo orodja »CA Identity Manager«

Diplomsko delo
na visokošolskem strokovnem študiju

izr. prof. dr. Miha Mraz
MENTOR

doc. dr. Mira Trebar
SOMENTOR

Ljubljana, 2008

Zahvala

Na tem mestu bi se rad zahvalil svojemu mentorju Petru Verunici za strokovno pomoč in veliko razumevanja pri izdelavi te diplomske naloge. Zahvala gre tudi mojemu mentorju na fakulteti za računalništvo in informatiko izr. prof. dr. Mihi Mrazu in somentorici doc. dr. Miri Trebar za vse konstruktivne pripombe in vso pomoč.

Vsebinsko kazalo

Kazalo slik

Seznam uporabljenih kratic

Kratica	Pomen	Slovenski prevod
AD	Active Directory	Aktivni imenik
CAFT	CA File Transfer	CA modul za pošiljanje datotek
CAM	CA Messager	CA modul za pošiljanje sporočil
CA-IM	CA Identity Manager	CA upravljanje identitet
CISO	Chief Information Security Officer	Predstojnik oddelka za informacijsko varnost
CLI	Command Line Interface	Vmesnik z ukazno vrstico
CMIP	Common Management Information Protocol	Protokol splošnih upravljalskih informacij
CPU	Central Processing Unit	Centralna procesna enota
CSV	Comma Separated Values	Vrednosti ločene z vejico
DSI	Distributed Security Integrator	Porazdeljeni združevalec varnosti
DSML	Directory Services Markup Language	Jezik za označevanje imeniških storitev
ESM	External Security Manager	Zunanji krmilnik za varnost
GUI	Graphical User Interface	Grafični vmesnik
HR	Human Resources	Človeški viri
HTTPS	Hypertext Transport Protocol Secure Sockets	Protokol, ki omogoča varno internetno povezavo
IAM	Identity and Access Managemt	Upravljanje identitet in dostopa
IM	Identity Manager	Upravljanje identitet
IT	Information Technology	Informacijska tehnologija
LAN	Local Area Network	Lokalno omrežje
LDAP	Lightweight Directory Access Protocol	Enostavni protokol za dostop do imenika
LPAR	Logical Partition	Logična particija (na mainframe sistemih)
ODBC	Open DataBase Connectivity	Odprta podatkovna povezljivost
PAM	Pluggable Authentication Module	Modul za integracijo z zunanjimi avtentikacijskimi rešitvami
PKI	Public Key Infrastructure	Infrastruktura za avtentikacijo s pomočjo javnega ključa
PM	Project Management	Upravljanje s projekti
RACF	Resource Access Control Facility	Orodje za nadzor pristopa k virom (na z/OS)
RBAC	Role Based Access Control	Kontrola dostopov na podlagi vlog
SAML	Security Assertion Markup Language	Jezik za označevanje z izjavo o varnosti
SAO	Solution Archicteture Overview	Pregled arhitekturne rešitve
SAS	Solution Architecture Specification	Specifikacija arhitekture rešitve
SNMP	Simple Network Management Protocol	Preprosti protokol za upravljanje omrežja
SoW	Statement of Work	Opis dela
SPML	Service Provisioning Markup Language	Jezik za logično opisovanje oskrbe uporabnikov
SSL	Secure Sockets Layer	Sloj varnih vtičnic
SSO	Single Sign-On	Enotna prijava
TLS	Transport Layer Security	Varnost transportnega sloja
UDDI	Universal description, discovery and integration	Univerzalni opis, odkrivanje in integracija
UPO	Universal Provisioning Option	Univerzalni oskrbni modul
USS	Unix System Service	Unix sistemski servis
XML	Extensible Markup Language	Razširljivi označevalni jezik

Povzetek

V današnjem času upravljanje vse večjega števila uporabniških identitet in dostopov do pomembnih vsebin predstavlja čedalje večji izziv velikim organizacijam. Zaradi tega obstaja na trgu veliko število različnih rešitev za upravljanje identitet in dostopov.

Večina rešitev ponuja odgovore zgolj na nekatera specifična vprašanja iz panoge upravljanja z identitetami in pristopi, manjše število vodilnih proizvajalcev programske opreme (CA Inc., IBM, Sun Microsystems, Novell) pa poskuša k navedeni problematiki pristopiti celovito, ker edino takšen pristop ustreza največjim organizacijam.

V svoji diplomski nalogi sem za problem rokovanja z identitetami uporabil orodje CA Identity Manager, rešitev za avtomatizacijo in upravljanje s storitvami, kot so kreiranje, spreminjanje in brisanje uporabniških računov in pravic v poslovno-informacijskih sistemih. Ker je tehnološki del rešitve v večji meri katalizator organizacijsko-procesnih sprememb kot logično samovsebovani informacijski sistem, sem kot osnovni tematski gradnik naloge postavil celovit projektni pristop. Pri tem mi je vodilni cilj prikazati osnovni življenjski cikel rešitve od snovanja do realizacije s poudarkom na spremembah, ki jih projekt terja na procesni in tehnični ravni.

Ključne besede: “identity management”, upravljanje uporabniških identitet, vloge, pravice

Abstract

In modern times, managing an ever increasing number of user identities and entitlements to important data is becoming a substantial challenge for large organizations. This has resulted in an onset of a large number of different identity and access management solutions.

Most of these solutions are targeted to address only specific functionalities within the larger realm of identity and access management, while a handful of major vendors (CA Inc., IBM, Sun Microsystems, Novell) opts for a holistic approach, as the only way to address the needs of the largest organizations.

In my diploma thesis, I have described the CA Identity Manager product, a solution for automation and management of user-oriented services such as creation, modification and deletion of user accounts and entitlements on IT business systems. Since the technical part of the solution serves predominantly as a cataliser of organizational/process changes and less as a self-contained information system, I have decided to use the project approach as the main building block of my thesis. My primary goal here was the solution's basic life cycle demonstration, with accent on the changes introduced by the project on process and technical layers, ranging from planning to realization.

Key words: identity management, user identity management, role, entitlement

1 Uvod

Z rastjo števila sistemov, čedalje večjo tržno dinamiko in vse bolj prisotnimi regulativnimi predpisi, vodenje in upravljanje velikega števila heterogenih uporabniških identitet in dostopov do pomembnih vsebin danes predstavlja vedno večji izziv sodobnim organizacijam.

Podati popolne informacije o uporabniku naj bi bilo enostavno opravilo, vendar pa pri upravljanju uporabniških identitet v zapletenih okoljih IT z več aplikacijami, različnimi platformami, operacijskimi sistemi in nezdružljivimi varnostnimi modeli, lahko postane težavno. Zahteve pri upravljanju in varovanju uporabnikov in njihovega dostopa niso bile nikoli večje.

Dodatna težava so sodobna okolja z velikim številom informacijskih sistemov, ki so med seboj bolj ali manj povezani. S povečanjem števila informacijskih sistemov se povečuje tudi število potrebnih preverjanj in s tem podatkovnih zbirk z atributi za identifikacijo in pravilno avtorizacijo uporabnika. V običajnih okoljih lahko srečamo 30 in več različnih mest, v katerih so shranjeni podatki o posameznem uporabniku. Vsak uporabnik v povprečju potrebuje dostop do petih informacijskih sistemov hkrati. Vendar večina organizacij nima zanesljivega sistema za določanje pripadnosti številnih uporabniških računov konkretnim uporabnikom – fizičnim ali pravnim osebam. Sistemi za upravljanje z identitetami zato omogočajo nadzor globalne uporabniške identitete in povezanih računov s centralnega mesta z uporabo avtomatiziranih in vnaprej pripravljenih postopkov ter pravil. Osnovni namen sistema je zagotoviti dostop do vseh potrebnih informacijskih virov v natančno določenih časovnih okvirih in z natančno določenimi pravicami. Sistem za upravljanje z identitetami posreduje vse potrebne informacije sistemu za upravljanje z dostopi, ki omogoči uporabniku vse potrebne parametre.

Vpeljava sistema za upravljanje z identitetami vedno sledi jasnim poslovnim zahtevam. Glavni razlogi, ki jih imajo podjetja za uvajanje sistema upravljanja z identitetami, so:

- zakonske in druge regulativne zahteve,
- zmanjševanje tveganj zaradi nedovoljenih dostopov do virov v podjetju ter zlorabe osebnih in zaupnih podatkov,
- zmanjševanje potrebnega časa pri postopkih zaposlovanja in s tem povezanih stroškov,
- podpora dostopa do aplikativnih rešitev za veliko število uporabnikov (zaposleni, partnerji, stranke ...),
- omogočanje vpogleda v vse atribute celotnega informacijskega sistema za posameznega uporabnika,
- poenostavitev oziroma avtomatizacija postopkov za dodeljevanje pravic uporabnikom in s tem zmanjšanje možnosti za napake.

Diplomska naloga temelji na zoženem obsegu dejanskega projekta uvedbe sistema za upravljanje z identitetami in pristopi izpeljanega v večji organizaciji iz finančnega sektorja. Pri tem je bilo težišče na področju upravljanja z identitetami, in sicer uvajanja avtomatizacije v do sedaj ročno izvajane procese.

CA Inc. je vodilno podjetje na svetovnem trgu rešitev za upravljanje z identitetami in pristopi, ki znotraj skupine "Identity and Access Management", ponuja centralizirane rešitve za upravljanje z identitetami, pristopi kritičnim virom (avtentikacija in avtorizacija), sisteme za enotno prijavo (SSO) ter revizijsko spremljanje varnostnih dogodkov, in sicer za "mainframe", porazdeljena (odjemalec-strežnik), spletna in heterogena ("mainframe-web") okolja.

V projektu smo želeli vpeljati avtomatsko izvajanje vseh korakov znotraj nalog upravljanja z identitetami in uporabniškimi računi s sprotnim zapisovanjem vseh rezultatov in odločitev v varno podatkovno bazo. Ker gre pri upravljanju z identitetami za enega od temeljnih infrastrukturnih servisov, je bilo potrebno izpolniti vrsto tehničnih in organizacijskih predpogojev za uspešno implementacijo.

Osnovni predpogoj za doseganje navedenih ciljev je bila izdelava globalne varnostne politike. Ta zajema definiranje vseh povezanih entitet, kot so organizacijska struktura, standardizacija delovnih mest, opisovanje in izboljšanje dosedanjih procesov upravljanja z uporabniki, določanje potrebnih odobritev in administrativnih pravic.

V prvem delu diplomske naloge je predstavljen problem naloge in poglobljen opis orodja "CA Identity Manager" in podrejenih tehnologij ter njihovih medsebojnih interakcij. Predstavljene so osnovne komponente, značilnosti ter operacije, ki temeljijo na uporabniškem odnosu do podjetja (zaposleni, dobavitelj, kupec, poslovni partner, itd.) in specifičnih pravicah znotraj organizacije. Zajete so tudi revizijske storitve, ki jih lahko uporabljajo interni in eksterni revizorji, z namenom ugotavljanja skladnosti z notranjimi politikami in zunanjimi regulativnimi predpisi.

V drugem delu naloge sem predstavil projektne korake - prehod na avtomatiziran sistem upravljanja identitet in določanja pravic in dostopa ter usklajevanje delovnega toka. Prikazane so izboljšave in prednosti uporabe rešitve CA Identity Manager. V skladu s ciljem projektno-usmerjenega ponazarjanja rešitve temu sledi še praktični del prikaza arhitekture rešitve in validacije uporabniških operacij z različnimi tipi testiranja.

2 Predstavitev problema

V današnjih organizacijah z velikim številom informacijskih sistemov, ki so med seboj povezani, so zahteve pri upravljanju in varovanju uporabnikov velike. S povečanjem števila informacijskih sistemov se povečuje tudi število potrebnih preverjanj in s tem podatkovnih zbirk z atributi za identifikacijo in pravilno avtorizacijo uporabnika. Večina teh operacij se izvaja ročno, kar ni zanesljivo in sledljivo ter je časovno potratno. Osnovni namen sistema je zagotoviti dostop do vseh potrebnih informacijskih virov v natančno določenih časovnih okvirih in z natančno določenimi pravicami.

2.1 Poslovne zahteve in cilji

Vodstvo organizacije se običajno odloči za izvedbo projekta upravljanja z identitetami na osnovi naslednjih poslovnih zahtev:

- **Skladnost s predpisi, ki jih mora organizacija upoštevati v roku 1-2 let.**
  Skladnost z delom regulativnih predpisov, ki se nanašajo na informacijsko varnost in razdeljevanje vlog (angl. *segregation of duties)* bo dosežena skozi aplikativno zagotovljeno izvajanje centralne informacijske varnostne politike in doseganje popolne transparentnosti pri razdeljevanju vlog, ki lahko pripeljejo do konflikta interesov. Izdelava poročil bo glavni mehanizem dokazovanja skladnosti.

- **Razbremenjevanje sistemskega osebja in zmanjševanje rasti stroškov dela.**
  Pri trenutni porabi človeškega dela za izvajanje nalog upravljanja z identitetami in računi, ter z vsemi s tem povezanimi mehanizmi preverjanja pravilnosti izvajanja teh procesov, obstoječe administrativno IT osebje nima dodatnega časa za procesne naloge s področja preverjanja in zagotavljanja regulativne skladnosti. Z avtomatizacijo ter beleženjem vseh uporabniških procesov bo osebje razbremenjeno.

- **Zmanjševanje nepričakovanih stroškov zaradi človeške napake.**
  Pri pomembnih procesih, kot je dodeljevanje dostopa do kritičnih sistemov, ni nezmotljivih kontrolnih mehanizmov, ki bi lahko preprečili pojavitev nenamerne ali namerne napake sistemskih skrbnikov. Tveganje, ki za organizacijo predstavlja varovanje osebnih in poslovnih podatkov osebja in strank, lahko terja izjemne sodne stroške in splošni padec zaupanja do organizacije. Zato se tvegani procesi avtomatizirajo z jasno sledljivostjo odgovornosti za vsak korak procesa.

2.2 Operativne zahteve in cilji

Projekt se izvaja v dveh fazah: analizi in implementaciji. Zaradi izjemne kompleksnosti tehnologije in organizacijskih procesov vseh zahtev ni možno opredeliti pred začetkom projekta. Zato prvi del projekta pokriva zapisovanje vseh formalnih in polformalnih procesov, vlog, poslovnih in aplikativnih posebnosti ter vseh ostalih dejavnikov, ki lahko vplivajo na uspešnost projekta. Zaradi kompleksnosti procesov se pričakuje, da bo prva faza zahtevala 60% skupnega trajanja projekta.

Osnovni cilji projekta so:

- Vzpostavitev centralnega imeniškega sistema, kot avtoritativne zbirke uporabniških podatkov. Shema LDAP (angl. *Lightweight Directory Access Protocol*) mora biti prilagojena trenutni organizacijski strukturi in dovolj fleksibilna, da sprejme vse pričakovane organizacijske spremembe v naslednjih treh letih.
- Izdelava registra vlog in opisovanje vseh relevantnih procesov v orodju Ares.
- Vzpostavitev infrastrukture in centralnega sistema za upravljanje z identitetami in na njih vezane uporabniške račune.
- Delegacija upravljanja z uporabniki v centralnem sistemu, razdeljena po vlogah in odgovornostih.
- Prilagajanje sistema delu z obstoječimi aplikacijami, zaradi centralizacije točk interakcije z uporabniškimi računi in podatki.
- Avtomatizacija vseh opisljivih in jasno definiranih postopkov upravljanja z identitetami in pravicami uporabnikov.
- Izdelava terminsko opredeljenih poročil po napotkih in zahtevah relevantnih regulativnih predpisov.
- Praktično spoznavanje s koncepti IAM in tehnologijami, zaradi pravilnega usmerjanja in doseganja čim večje koristi v nadaljnjih korakih.

2.3 Projektni cilji

Natančni projektni koraki in njihovi lastniki se precizno opredeljujejo v projektnem planu. Navedeni so osnovni projektni koraki do dveh ravni granulacije:

- **Planiranje in postavitev infrastrukture:**
    - Izdelava opisa dela in priprava dokumentacije za upravljanje projekta.
    - Podroben posnetek stanja (delavnice in pogovori), skiciranje rešitve.
    - Izdelava scenarijev in usklajevanje z zahtevami.
    - Razvoj temeljne dokumentacije (SAS).
    - Pregled in namestitev strojne in programske opreme, mrežne postavitve.
    - Konfiguracija operacijskih sistemov, aplikacijskega strežnika in podatkovnih baz.
    - Namestitev orodja “CA Directory”.
    - Namestitev komponent “CA Identity Manager”.
    - Osnovno povezovanje komponent.
- **Konfiguracija in testiranje:**
    - Konfiguracija podatkovnih baz IM (“Workflow, Task Persistence, Audit, Reporting”).
    - Kreiranje in uvažanje sheme LDAP.
    - Konfiguracija vmesnika za oskrbo “Active Directory” uporabnikov.
    - Konfiguracija vmesnika za oskrbo uporabnikov na dodatnih aplikacijah.
    - Razvoj skript za polnjenje uporabniškega repozitorija z obstoječimi podatki.
    - Definiranje politike za oskrbo AD uporabnikov.

- Definiranje politik za oskrbo uporabnikov na dodatnih aplikacijah.
- Konfiguracija "Universal Feed Option"-a za polnjenje imenika s podatki o obstoječih uporabnikih.
- Populacija direktorija.
- Korelacija in preverjanje pristnosti podatkov na podlagi matične številke na ravni skupine in uporabniškega imena ("Explore and Correlate").
- Konfiguracija in prilagajanje vmesnika "Identity Manager".
- Ustvarjanje politik za segregacijo dolžnosti.
- Prilagajanje osnovnih poročil (dodajanje, spreminjanje, deaktivacija, reaktivacija, brisanje).
- Validacija funkcionalnosti.
- Validacija odzivnosti.
- Validacija uporabniških scenarijev.
- Izdelava plana za prehod v produkcijo in scenarija, ki se nanaša na ponovno vzpostavitev računalniškega sistema (angl. *fallback*).
- Prehod v produkcijo.
- Demonstracija administracije.
- Razvoj skript za bremensko testiranje (angl. *load testing*).
- Bremensko testiranje.
- Post-projektni posnetek stanja.
- Dokumentacija nalog.
- Dopolnjevanje in primopredaja dokumentacije.
- Primopredaja projekta.

2.4 Pregled ocene trenutnega stanja

Trenutno stanje (stanje pred implementacijo rešitve) je rezultat evolucijskega razvijanja organizacijskih procesov na temelju poslovnih izzivov in tehničnih ter človeških virov skozi daljše časovno obdobje. Osnovne storitve s področja upravljanja z računi že obstajajo, ampak se skoraj v celoti izvajajo ročno. Trenutno ne obstaja globalna politika in na njej zasnovani procesi krmiljenja in nadzora teh storitev.

Ker ta projekt predstavlja prvi globalni poskus reševanja problema upravljanja z identitetami, trenutni procesi niso konsistentni znotraj celotne organizacije.

Osnovne značilnosti trenutnega stanja so naslednje:

- Procesi in politike za upravljanje z uporabniki in gesli se izvajajo ročno.
- Predstojnik oddelka za informacijsko varnost (angl. *CISO*) je odgovoren za upravljanje dostopov, vendar pa ne obstajajo procesni mehanizmi za uveljavljanje skladnosti s standardi.
- Odobritev in usmerjanje na novo zaposlenega in sprememba uporabniškega računa se opravljajo ročno (e-pošta, fax, telefon), brez zagotovljene revizijske sledi sprememb.
- Procesi v primeru zahteve novih pravic, izgube gesla ali prijave na novo storitev nimajo jasno definiranih lastnikov.
- Generiranje uporabniških računov, spreminjanje poročil in pregled pravic so ročni procesi.
- Upravljanje z gesli je avtomatizirano v nekaterih sistemih. Administracijo gesel izvaja služba za pomoč uporabnikom ali končni uporabniki. V primeru problemov se

zahteve za ponastavitev gesla pošiljajo sistemskemu administratorju, ki jih rešuje ročno.
- Izdelava poročil o pravicah uporabnikov in pristopih k kritičnim sistemom zahteva dodatno ročno delo, ki je izpostavljeno možnostim napake zaradi človeških dejavnikov.

2.5 Trenutno obstoječi procesi

Temeljni procesi, ki so bili opisani in dokumentirani so naslednji:

- Novi zaposleni
- Novi zunanji sodelavec
- Revizija varnosti
- Zahteva uporabniškega dostopa
- Odstranitev uporabnika
- Novi strežnik/aplikacija
- Definiranje politik
- Ponastavitev uporabniškega gesla

Odkrito je bilo, da imajo navedeni procesi številne izjeme v različnih organizacijskih vejah in posebnih primerih. Zato dokumentirani procesi predstavljajo idealni skupni presek korakov, ki bo veljal kot standard pri implementaciji rešitve.

Razlaga pojmov zaposleni in zunanji sodelavec:

Zaposleni – katerakoli oseba, ki dela za organizacijo in ima odobren fizičen dostop do virov, uporabo telefona, računalnika. Lahko je zaposlen za nedoločen čas ali pogodbeno.

Zunanji sodelavec – partner, kupec, izvajalec, ki mu je odobren dostop do poslovnih aplikacij, vendar ne do infrastrukture IT sistemov. Zunanji sodelavec je angažiran v projektih.

2.5.1 Novi zaposleni

Dodajanje novega zaposlenega se izvaja tako, da kadrovska služba (angl. *Human Resources*) dodaja novega uporabnika po prihodu v podjetje. Poslovni skrbnik kot nadrejena oseba novega zaposlenega, pošilja zahteve za dodeljevanje:

- IT operacij:
  - LAN
  - E-pošta
- Sredstev:
  - dostop do stavbe
  - zagotavljanje delovne mize
  - namestitev telefona

Skrbnik aplikacije nato namesti poslovno aplikacijo, uredi uporabniški račun in potrebne dostope za posel. Skrbnik varnosti uredi dostope do sistema za upravljanje z gesli. Vse naštete zahteve se rešujejo s telefonom ali s faxom in niso avtomatizirane, niti sledljive.

Uporabnik mora dobiti ustrezna dovoljenja (angl. *credentials*) za dostop do računov. Dovoljenja se preverja na podlagi avtentikacije, opravljene z geslom ali overilnim/avtentikacijskim žetonom, ključem ali katerokoli drugo metodo.

2.5.2 Novi zunanji sodelavec

Dodajanje novega zunanjega sodelavca se začne s "sponzorstvom" skrbnika strank in partnerjev, ko zunanji sodelavec, partner, kupec ali pogodbenik-naročnik potrebuje dostop do virov podjetja. V tem primeru z zunanjim sodelavcem ne upravlja kadrovska. Zahteve za dostop se izvršujejo preko skrbnika strank in partnerjev preko e-pošte ali faxa. Zunanjemu sodelavcu se dodeli uporabniško ime in geslo za dostop do določenih virov, vnaprej dogovorjenih s skrbnikom strank in partnerjev.

2.5.3 Revizija varnosti

V sistemu se revizijske funkcije izvajajo po določenem urniku. To se nanaša na interno in eksterno revizijo. Revizorji potrebujejo poročilo o uporabniškem dostopu, zaradi preverjanja pravic dostopov uporabnikov ter preverjanja uporabniške pravice in spremembe računov. Proces izločevanja uporabnika iz kadrovskega sistema poteka ročno, kot tudi proces zbiranja in priprave seznama izvajalcev in drugih zunanjih sodelavcev. Proces zbiranja informacij uporabniških računov poteka sistemsko v določenem času. Poročilo o uporabniškem računu, poročilo o pravicah in poročilo o spremembah so predloženi ročno. Pri detekciji neavtoriziranih uporabniških računov je proces brisanja računov ročen in se ne beleži v sistemu.

2.5.4 Zahteva uporabniškega dostopa

Zahteva uporabnika za dostop se odvija ročno in je večinoma sprožena na pobudo končnega uporabnika in to v dveh primerih:

- Zahteva dostopa do dodatnih virov v primeru nove službe.
- Zahteva za pomoč v primeru težav pri dostopu do sistema.

Uporabnik pošlje zahtevo po faxu ali e-pošti. Zahtevo mora odobriti uporabnikov skrbnik, ki je za:

- zaposlene praviloma uporabniški skrbnik ali nadrejeni,
- zunanje sodelavce praviloma skrbnik partnerjev in strank.

Po tej odobritvi mora to zahtevo odobriti aplikacijski skrbnik v IT oddelku in jo izvršiti v sistemu.

2.5.5 Odstranitev uporabnika

V sistemu se odstranitev uporabnika izvaja tako, da kadrovska služba ročno zbriše uporabnikove podatke, ko zaposleni zapusti podjetje. V primeru zunanjih sodelavcev (kupci, partnerji in ostali), ki ne potrebujejo več dostopa, skrbnik strank in partnerjev ročno ažurira seznam ali bazo z dovoljenji. Za odstranitev uporabniških računov je potrebno poslati uradno obvestilo lastniku poslovnega procesa. Odstranitev uporabniških virov je tudi ročen proces katerega mora odobriti poslovni skrbnik. V tem primeru je potrebno poslati uradno obvestilo

za odstranitev dostopa do podjetja in prostorov ter naprav, medtem ko je vrnitev računalnika odvisna od poslovnega skrbnika IT oddelka.

Dogaja se, da se uradno obvestilo ne procesira naprej, tako da lahko pride do "ghost" računov, ki jih ne odkrijejo vse do periodične varnostne revizije. "Ghost" računi predstavljajo vse račune, ki so ostali aktivni tudi po preteku opravljanja funkcije, na podlagi katere so bili uporabniku dodeljeni.

2.5.6 Novi strežnik/aplikacija

Pri razvijanju aplikacij se zahteva operativni vodič (angl. *Operational Guide*), ki omogoča administracijo skrbniku aplikacij. Operativni vodič vključuje upravljanje z uporabniškimi računi, kar je odgovornost razvojnega skrbnika. Ko se postavljajo novi strežniki, je vodja IT operacij odgovoren za njihovo upravljanje, kar vključuje tudi upravljanje uporabniških računov.

2.5.7 Definiranje politik

V obstoječem sistemu so definirani procesi za upravljanje računov in obstajajo lastniki za vsak proces. Definirani so tudi standardi nastavitve gesla. Trenutno ne obstaja periodičen pregled procesov za politiko in standarde ter ne obstajajo procesi in standardi za celotno upravljanje z identitetami podjetja.

2.5.8 Ponastavitev uporabniškega gesla

Ponastavitev uporabniškega gesla se rešuje v primeru zahteve za pomoč končnega uporabnika, če ima težave z dostopom do sistema. Služba za pomoč uporabnikom skuša rešiti težavo s ponujanjem nasvetov in napotkov. Če gre za težavo z gesli, se uporablja sistem za upravljanje gesel, ker drugače nima dostopa do sistema, da bi omogočila iskanje in odpravljanje napak. V primeru, da ponastavitev gesla ne deluje, se zahteva pošlje tehnični podpori.

3 Opis uporabljenega orodja

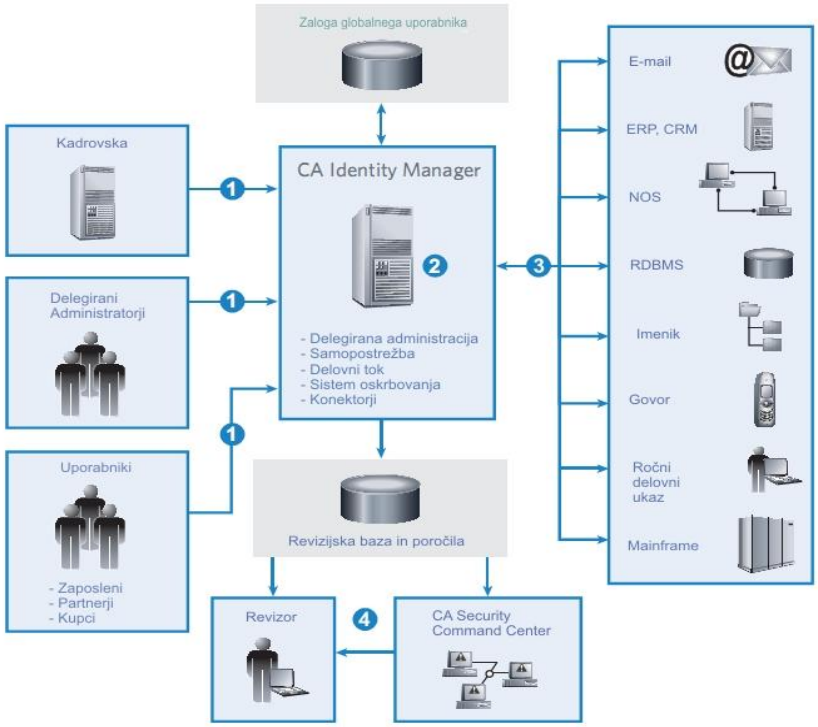
CA Identity Manager je programsko orodje za avtomatizacijo in upravljanje z identitetami. Sestavljen je iz modulov CA Admin in CA Directory.

3.1 Upravljanje identitet z orodjem CA Identity Manager

CA Identity Manager (CA-IM) omogoča avtomatično upravljanje s storitvami, kot so kreiranje, spreminjanje in morebitno brisanje uporabniških računov in pravic na poslovnih sistemih. Te operacije temeljijo na uporabnikovi zvezi s podjetjem (zaposleni, dobavitelj, kupec, poslovni partner, itd.) in specifičnih pravicah znotraj organizacije [1]. Poleg tega omogoča tudi revizijske storitve, ki jih lahko uporabljajo interni in eksterni revizorji za ugotavljanje skladnosti z notranjimi politikami in zunanjimi regulativnimi predpisi.

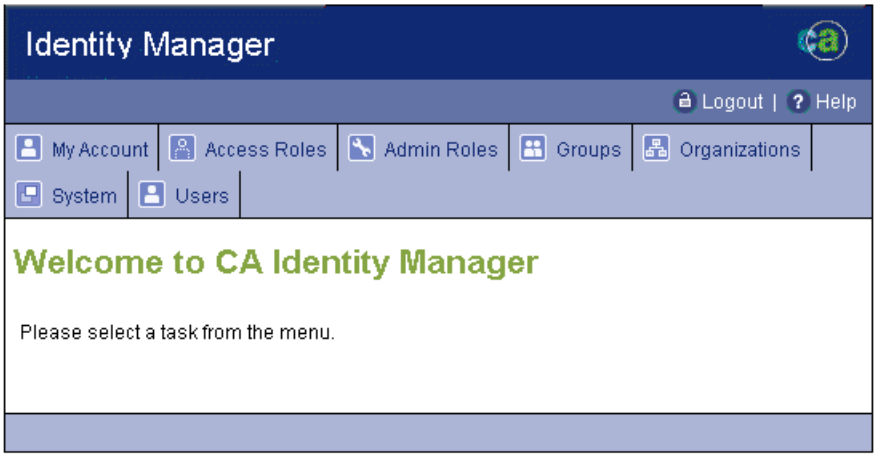
Koraki procesa so prikazani na sliki 1:

1. Računi, pravice ali zahteve za spremembo gesla se pošiljajo do CA Identity Managerja bodisi preko avtomatizirane povezave s kadrovskim sistemom, preko zahtev pooblaščenih administratorjev, ali preko končnih uporabnikov.
2. CA Identity Manager začne delovni tok, izvede vsa potrebna preverjanja in odobritve, določi učinek na ciljne sisteme in upravlja s spremembami na ciljnih sistemih.
3. Avtomatične spremembe ciljnega sistema se izvedejo.
4. Vse spremembe so zapisane, revidirane in pregledane s strani varnostnega in revizijskega osebja.



- **Slika 1. Umestitev programskega okolja v delovno okolje.**

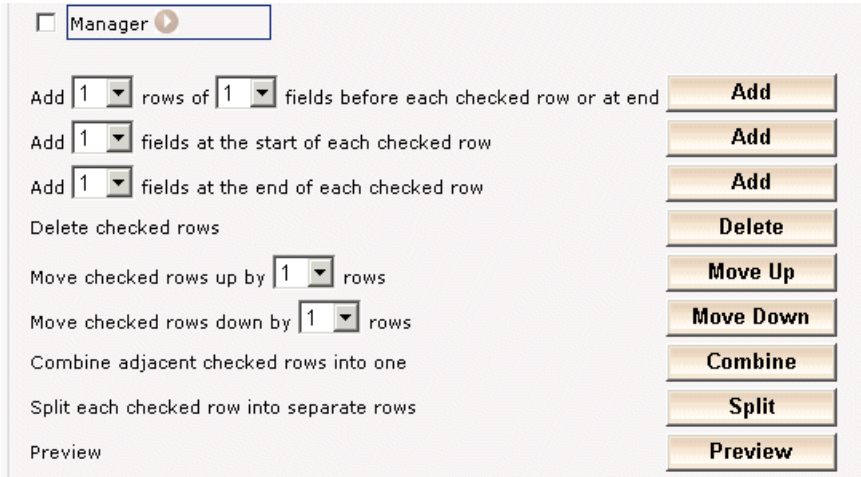
3.1.1 Značilnosti orodja CA Identity Manager



- **Slika 2. Osnovni meni orodja CA Identity Manager.**

Ker so zahteve in procesi vsake organizacije različni, osnovni vmesnik Identity Managerja v nobenih dveh primerih ni videti enako. Zasnovan je kot portalna aplikacija (slika 2), ki vsakemu udeležencu ponuja izbirnike, ki mu omogočajo opravljanje ravno tistih nalog, za katere je odgovoren in pooblaščen [2].

Na sliki 3 vidimo primer spletnega nastavljanja videza in vsebine vmesnika za določeno vlogo.



- **Slika 3. Namestitev začetnega vmesnika orodja CA Identity Manager.**

Ključne značilnosti orodja CA Identity Manager so [1]:

- *Delegirana uporabniška administracija* – Razdeljevanje pooblastil za uporabniško administracijo omogoča IT organizacijam selektivno porazdeljenost uporabniško-administrativnih nalog tistim osebam in skupinam, ki so najbolj primerne za izvajanje tovrstnih organizacijskih storitev. Upravljanje z določenimi administrativnimi procesi se lahko dodeli skupinam znotraj ali zunaj podjetja. Nadzorovana delegacija uporabniške administracije lahko dramatično izboljša zmožnosti vodenja oddelka IT

in drugih organizacijskih enot. Poleg tega omogoči tudi dodaten nivo varnosti, preglednosti in osebne odgovornosti.

- *Samopostrežna administracija* – CA-IM ponuja visoko prilagodljiv administrativni vmesnik, ki temelji na portalni tehnologiji in ga uporabljamo z internetnim brskalnikom. Vmesnik uporabnikom omogoča upravljanje z lastnim profilom, geslom in pravicami, seveda, če organizacijska varnostna politika predpisuje to možnost ter je znotraj okvirjev globalne varnostne politike.

- *Integrirana podpora za delovne procese* – omogoča vpeljavo in hkratno avtomatizacijo vseh uporabniško-administrativnih procesov ter poskrbi za postavitev prilagodljive platforme za podporo enotnemu načinu vodenja uporabniške administracije za sleherno uporabniško skupnost. Le-ta lahko zajema serijske in paralelne procese, večstopenjske odobritve in možnost delegacije pravic.

- *Upravljanje z gesli* – globalni proces upravljanja z gesli zagotavlja večjo varnost v organizaciji skozi aplikativno vpeljavo nominalnih varnostnih predpisov. CA-IM zagotavlja storitev za upravljanje z gesli, ki vsebuje samopostrežno upravljanje, podporo za pozabljena gesla, dvosmerno sinhronizacijo gesla, centralizirano skupino pravil, prilagodljivo uporabo politike upravljanja z gesli, Microsoft GINA podporo in avtomatično periodično spreminjanje gesla, če upoštevamo pravila minimalne kompleksnosti.

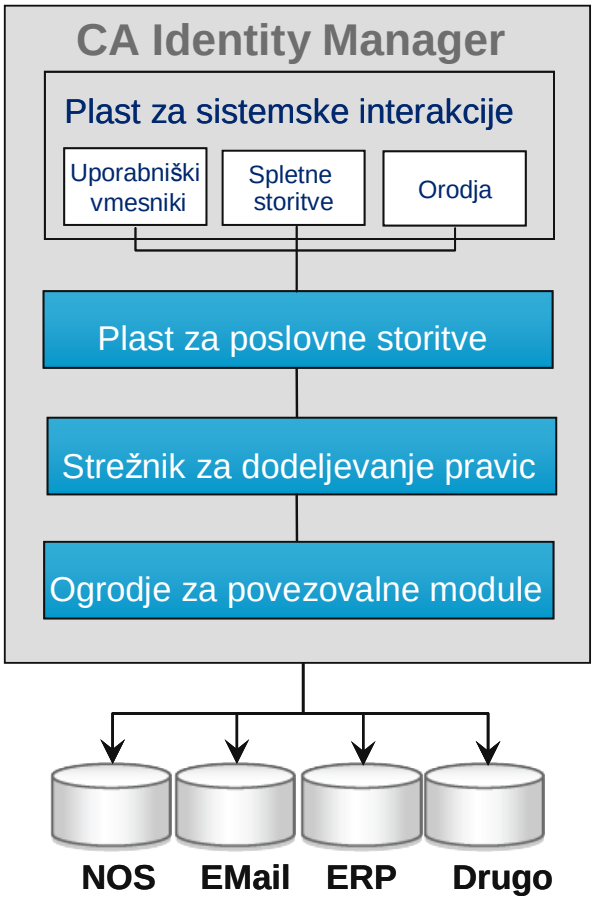
- *Strukturirani model upravljanja* – model CA-IM upravljanja z uporabniki ponuja strukturiran in prilagodljiv model za uporabniške in administratorske vloge in upravljanja z odgovornostjo. Ta model vpliva na ključne entitete kot so vloge, pravila, skupine, organizacije, opravila in nadzor dostopa po funkcijah RBAC (angl. *Role Based Access Control*) ali kontrole dostopov na podlagi vlog.

- *Integrirano doseganje skladnosti z regulativnimi zahtevami* – Ob aplikativni vpeljavi regulativnih predpisov in upoštevanju segregacije in certifikacije pravic CA-IM omogoča doseganje skladnosti skozi ustrezno definirane poslovne procese, vključno z vpeljavo osebne odgovornosti, poročanjem o ključnih metrikah in relevantnih dogodkih, ter omogočanjem revizijskega vpogleda v trenutno stanje in pretekle dogodke.

- *Odprti vmesnik* – zaradi zagotavljanja uporabnosti v velikih, heterogenih okoljih mora proces upravljanja identitet sodelovati s številnimi različnimi sistemi. Zaradi tega CA-IM zagotavlja veliko število odprtih vmesnikov, kot so podpora za SPML (angl. *Service Provisioning Markup Language*), SAML (angl. *Security Assertion Markup Language*), C in Java API, vmesnik za spletne servise in XML/CSV (angl. *Extensible Markup Language/ comma-separated values*).

3.1.2 Tehnični vidiki orodja CA Identity Manager

Tehnični vidiki orodja CA Identity Manager vsebujejo štiri osnovne plasti in so predstavljeni na sliki 4.



- **slika 4. Tehnični vidiki orodja CA Identity Manager.**

Prva je plast za sistemske interakcije, ki vsebuje uporabniške vmesnike, spletne storitve in orodja. Plast za poslovne storitve skrbi za poslovne vloge, skrbniške vloge, politike, delovne procese, zapisovanje dogodkov, življenjski cikel nalog in elektronska obvestila (e-pošta). Sledi strežnik za dodeljevanje pravic *(angl. provisioning server),* ki skrbi za virtualizacijo, sinhronalizacijo ter korelacijo in preverjanje (angl. *explore & correlate*). Temu sledi ogrodje za povezovalne module in povezovalni moduli (konektorji) za upravljanje z objekti in uporabniško zbirko, iskanje ter agenti za upravljanje z gesli [2].

3.1.3 Prednosti uporabe orodja CA Identity Manager

Glavna prednost uporabe orodja CA Identity Manager je zmanjševanje stroškov s pomočjo avtomatizacije in delegacije uporabniške administracije ter sprostitev ročnih nalog in opravil sistemskih administratorjev. Temu sledi zvišanje varnosti z avtomatično in centralizirano vodeno politiko uporabniške administracije, ki zagotavlja, da ima uporabnik pravico dostopa le do tistih virov, ki jih po trenutni delovni vlogi potrebuje in ob tem ne nabira odvečnih dostopov do sistemov med premikanjem po različnih organizacijskih vlogah. Avtomatizirana uporabniška administracija zagotavlja, da samo pooblaščene osebe lahko dostopajo do občutljivih sistemov, upoštevajoč ključne varnostne kontrole, kot je porazdelitev nalog (angl. *segregation of duties*). Obširno zapisovanje, korelacija in poročanje o relevantnih varnostnih politikah in incidentih omogočajo doseganje skladnosti z internimi in eksternimi varnostno-regulativnimi zahtevami. CA-IM sistem pomaga vzpostaviti tri glavne stebre vseh regulativnih zahtev:

1. Upravljanje z uporabniki in pravicami v kontroliranem okolju.
2. Upravljanje z IT sistemi v kontroliranem okolju.
3. Zagotovljanje varnosti osebnih podatkov.

3.1.4 Ciljne organizacije

Ciljne organizacije za uporabo orodja CA Identity Manager so velike organizacije (finančni sektor, telekomunikacije, vlada, visoko razvite organizacije), organizacije s heterogenimi tehnologijami ("mainframe", unix, windows, splet, strežnik-odjemalec), organizacije z velikim številom uporabnikov (zaposleni, stranke in partnerji) ter organizacije usmerjene v ponudbo spletnih storitev.

3.2 Modul CA Admin

Modul CA Admin je temeljna logična komponenta orodja CA Identity Manager za dodeljevanje, spreminjanje in odvzem pravic [3]. Avtomatizira dodeljevanje pravic, odvzem pravic ter upravljanje z gesli na različnih sistemih, aplikacijah, fizičnih virih in spletnih storitvah. Podpira raznovrstne konektorje in standardna orodja za upravljanje in varnost v IT okoljih.

Potrošniki, partnerji in zaposleni pričakujejo poosebljene spletne storitve z visoko dostopnostjo. V želji, da povečajo število in kakovost procesov in funkcij ter izboljšajo dostop do aplikacij, organizacije nehote povečujejo tveganja, povezana z upravljanjem dostopov. Količina in poslovna vrednost osebnih informacij, shranjenih v zbirki, združena z vseprisotno odprto naravo interneta, je spodbudila organizacije, da povečajo zaščito pred neavtoriziranim dostopom do njihovih kritičnih podatkov.
"IT na zahtevo" kot koncept drastično povečuje potrebo po kontroliranem upravljanju z identitetami in dostopi, možnostih popolnega revizijskega vpogleda in aplikativno upravljane varnostne politike. Čedalje večja uporaba spletnih storitev in potreba po varnosti in zaščiti podatkov ter vsebin je rezultirala v velikem številu osebnih identitet. Vzrok za to je iskati v tem, da vsaka aplikacija lahko zahteva svoj ID, geslo in svoja pravila upravljanja za avtentikacijo uporabnika.

Zato današnjemu uporabniku predstavlja vse večji izziv pomnjenje oziroma varno hranjenje vse večjega števila gesel. Dodaten izziv predstavlja tudi ročno spreminjanje, preverjanje in resetiranje gesla, ki povečuje administrativne stroške. Podatki potrjujejo, da 30 % vseh klicev v center za pomoč uporabnikom obsega ponastavitve/resetiranje gesla. Drugi podatki kažejo zmanjševanje produktivnosti, ko uporabnik ne more dostopati do zahtevanih storitev v trenutku, ko jih potrebuje. Bistven element upravljanja z identitetami in dostopi je zagotavljanje dostopa do ustreznih sistemov z ustreznimi pravicami s strani zaposlenih, strank, partnerjev in dobaviteljev.

CA Admin ustvarja račune z ustreznimi pravicami na različnih sistemih, fizičnih virih in spletnih storitvah s polno avtomatizacijo ter avtomatično odvzema pravice odpuščenim zaposlenim in začasnim delavcem, ki so se jim pogodbe iztekle. S tem se eliminirajo mrtvi računi in se zmanjšuje izpostavljena površina za morebitne napade. Zagotavlja dostop do občutljivih in pomembnih podatkov le avtoriziranim uporabnikom, poleg tega jim omogoča obsežen sistem zapisovanja in poročanja do katerih virov je uporabnikom dovoljen dostop. To je omogočeno z inherentnimi mehanizmi zapisovanja dogodkov ter z izdelavo poročil na

podlagi podatkov v interni relacijski podatkovni bazi. Za poročanje se lahko uporabljajo priložena orodja, ali katerokoli drugo orodje drugih proizvajalcev, ki je zmožno brati preko ODBC standarda. CA Admin skrbi za sinhronizacijo gesel in izboljšuje varnost z zmanjševanjem možnosti napake človeškega dejavnika.

3.2.1 Značilnosti modula CA Admin

Značilnosti modula CA Admin so [3]:

- *Vloga in politika uporabniške administracije*

  Modul upravlja z uporabniki v skladu z njihovo funkcijo. Na ta način kontrolira dostop do zahtev in storitev, ki jih določeni uporabnik potrebuje v sistemu. Shranjuje vse uporabniške račune v strogem skladu s politiko korporacije. Na podlagi uporabnikove delovne vloge ustvarja, spreminja in ukinja uporabniške račune v heterogenih sistemih. Izvršuje celovito administracijo vseh uporabniških pravic za IT račune in fizične vire. Podpira integracijo imenika z enostavnim protokolom LDAP (angl. *Lightweight Directory Access Protocol*) za dostop do imeniškega servisa. Generična opcija LDAP omogoča integracijo z direktorijem LDAP ali aplikacijo načrtovanja avtoritativnih virov uporabniških informacij. ODBC (angl. *Open Database Connectivity*) odprta podatkovna povezljivost omogoča integracijo s sistemom, ki uporablja relacijske podatkovne baze kot zbirko uporabniških informacij. Pri vnosih iz kadrovskega sistema v modul CA Admin za delovne procese se vsi računi avtomatično kreirajo in ažurirajo. Spremembe v kadrovskem sistemu se avtomatično reflektirajo v modulu CA Admin in se hranijo s statusom zaposlenega.

- *Samopostrežna podpora*

  Modul omogoča uporabniku resetiranje in odklepanje gesel in računov, pregledovanje in upravljanje z informacijami. Vsebuje visoko nastavljiv mehanizem klic-odziv (angl. *challenge/response*), ki omogoča organizacijam vzpostavitev samopreverjanja v skladu z natančnimi predpisi.

- *Integracija s CA Security Command Centrom*

  Beleženje dostopov in varnostnih dogodkov je pomemben temelj v strategiji upravljanja varnosti dostopa. Dogodki se lahko procesirajo in združijo v celovito revizijsko sliko.

3.2.2 Operativne razširitve

Operativne razširitve modula CA Admin so dvosmerna sinhronizacija gesel in časovno zasnovani ukrepi. V modulu CA Admin je omogočanje, onemogočanje in brisanje ukrepov lahko vodeno po časovnem atributu. Globalni uporabniki, pravila in pravice se lahko preimenujejo in prestavljajo. Te operacije so podprte tudi v prilagojenem imenskem prostoru [5].

3.2.3 *Administrativne razširitve*

Administrativna razširitev modula CA Admin ponuja dva načina upravljanja z administrativnimi privilegiji:

- Globalno ustvarjanje ciljnih skupin – politike se vežejo na ročno definirane skupine.
- Dinamično ustvarjanje ciljnih skupin – politike se vežejo na dinamično ustvarjene skupine (po določenem kriteriju na podlagi imeniških atributov).

Vgnezdena pravila, skupine in administratorski profili omogočajo uporabnikom združevanje vlog, ki pripadajo drugi specifični vlogi. Npr. globalna skupina uporabnikov se lahko vgnezdi v drugo globalno skupino uporabnikov, administratorski profil pa se lahko vgnezdi v drugi administratorski profil.

Razširitvene opcije so narejene v modulu CA Admin za naslednja okolja:

- Microsoft Active Directory,
- CA Access Control,
- Microsoft Excange 5.5,
- Microsoft Excange 2000,
- IBM Lous Notes Domino,
- Oracle,
- OS/400,
- SAP,
- UNIX.

3.2.4 *Podprte platforme*

Na sliki 5 vidimo platforme, ki jih trenutno podpira modul CA Admin. Med naštetimi je večina danes najbolj uporabljanih platform s strani manjših, kot tudi zelo velikih organizacij.

Supported Platforms

*e*Trust Admin Options				
Operating Systems	**Groupware**	**Databases**	**ERP Applications**	**Generic**
Windows NT, 2000, 2003	Exchange 2000	IBM DB/2	Oracle e-Business Suite	Universal Feed
Linux: Red Hat, SuSE	Exchange 5.5	Informix	PeopleSoft	SAP
Linux for OS/390	Lotus Notes Domino	Advantage™ Ingres®	SAP	ERP Applications
SUN Solaris	Novell Bindery	Active Directory/ ADAM		
HP-UX	Novell NDS	MS SQL		
HP Safeguard		Sybase		
IBM AIX		Oracle		
Tru 64		Enterprise Relational Database		
IRIX				
AS/400				
NSK Safeguard Open VMS, S/390, Z/OS, AS/400				

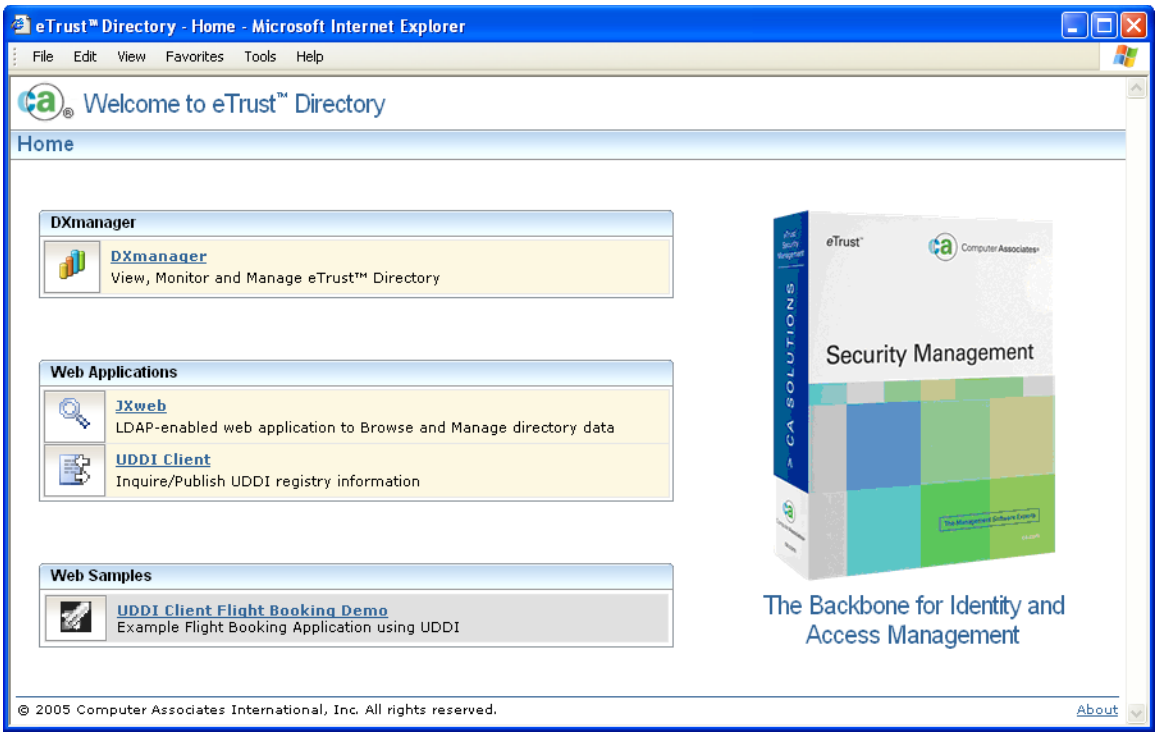
*e*Trust Admin Options	
Operating Systems	**Mainframe**
Microsoft Windows 2000/2003 Server	*e*Trust CA-ACF2
	*e*Trust CA-Top Secret
	IBM RACF

- **Slika 5. Osnovne platforme, ki jih podpira CA Admin.**

3.3 Modul CA Directory

Modul CA Directory je "hrbtenica" imeniškega servisa. Ponuja visoko stopnjo razpoložljivosti, zanesljivosti, razširljivosti in zmogljivosti. Na sliki 6 vidimo osnovni CA Directory vmesnik. Platforme, ki jih podpira, so naslednje: Windows 2000-SP4+, XP 5.1 SP1+, 2003, Sun Solaris 7,8,9, Linux/Intel Red Hat 8.0,9.0, AS3.0 Suse 9, HP-UX 11.0, IBM AIX 5.1 [6].

Današnje hitro spreminjajoče se poslovno okolje vpliva na podjetja tako, da omogočajo strankam, zaposlenim in poslovnim partnerjem heterogene storitve. Za uporabnike morajo biti te storitve čim bolj enostavne, poosebljene za uporabo in varovane. Za organizacije morajo biti te storitve hitre, vedno dostopne in sposobne ponuditi visoko ravnen neprekinjenega delovanja. Določene informacije in podatki morajo biti vedno na razpolago kot podpora tem številnim sistemom. Bančni ali vladni spletni portali morajo trenutno in zanesljivo avtenticirati uporabnike in postreči s poosebljenim delovnim prostorom in nastavitvami. Ponudniki digitalne televizije in internetnega dostopa morajo biti sposobni v realnem času spremljati servise in storitve, do katerih naročnik lahko dostopa. Imeniki in repozitoriji, v katerih se shranjujejo kritične informacije in pravice, so osnova za nemoteno in varno ponujanje omenjenih storitev. Zato največji izziv predstavlja ponujanje teh rešitev s podanimi zahtevami znotraj opredeljenih servisnih ravni (angl. *service level*).



- **Slika 6. Vmesnik CA Directory.**

3.3.1 *Posebne značilnosti in funkcije*

Posebne značilnosti in funkcije modula CA Directory so [5]:

- *Razširljivost in zmogljivost*

Neodvisni primerjalni poskusi pokažejo, da je CA Directory najhitrejši med tovrstnimi rešitvami. Modul CA Directory lahko procesira/obdela 10.000 zahtev na sekundo na enem 2GHz CPU, kar je do 20 krat hitrejše kot ostali znani imeniki. Takšen rezultat z znatnim prihrankom strojne opreme je lahko dosegljiv na veliko šibkejši strojni opremi, kot pri ostalih produktih. Podjetje ga je testiralo na več kot 500 milijonov uporabnikih in milijardi vnosov. Lahko meri več deset milijonov vnosov vertikalno na enem samem strežniku, horizontalno pa, povezujoč število strežnikov v X.500 shemi, se zmogljivosti linearno povečujejo.

- *Razdeljevanje in usmerjanje*

Ena od glavnih značilnosti modula CA Directory je možnost podpore visoko porazdeljenim okoljem brez izgube zanesljivosti ali zmogljivosti. Hitro preklapljanje in usmerjanje skrbi za inteligentno in pregledno veriženje zahtev porazdeljenega strežnika. To omogoča aplikaciji, da vidi imenik kot enotni logični hrbtenični imenski sistem, ne glede na število strežnikov. V repliciranem okolju CA Directory lahko avtomatično in transparetno usmerja zahteve do alternativnih strežnikov v primeru, da stroji odpovejo. To je ključna lastnost za zagotavljanje stalne dostopnosti. Navidezni imenik modula dovoljuje tudi integracijo obstoječih LDAP strežnikov v porazdeljeni imenik hrbtenice. Možnost integracije logičnih LDAP „otokov“ v en sam navidezni imenik lahko poenostavi podjetniško administracijo.

- *Replikacija/ponavljanje in zanesljivost*

Modul CA Directory je edini imenik, ki podpira večsmerno “multi-master” replikacijo v realnem času. To omogoča varno porazdelitev obremenitev in takoj prestavi trenutne zahteve na alternativne strežnike v primeru izpada naprave ali omrežja. Ima inteligenten sistem nadomestitve načina delovanja in ponovne vzpostavitve. Če strežnik izpade, drugi strežnik prevzame opravilo brez izgub storitve. Ko se povrne izpadli strežnik, se avtomatično pridruži hrbtenici. Večina produktov določa “master-slave” ali “dual master” replikacijo, kar omejuje njihovo možnost razširitve in replikacije. Modul CA Directory ima simetrično “multimaster” replikacijsko shemo, ki omogoča poljubnemu številu strežnikov medsebojno replikacijo.

- *Napredna varnost*

Modul CA Directory vsebuje veliko varnostnih rešitev za podporo varnih aplikacij, kot so sistemi za upravljanje identitet in dostopa, strežniki za enotne prijave, spletni portali in napredne UNIX avtentikacije. Lahko uporablja X.509 certifikate in “Hardware Security” module za varne avtentikacije uporabnika. Zagotavlja “rule based” in “role based” kontrolo dostopa za zaščito informacij, virov, aplikacij in profilov. Lahko uveljavi razsežna pravila za gesla, kar je zelo pomembno za podjetja z visokimi varnostnimi zahtevami. Podpira najbolj razširjene industrijske standarde, kot sta Secure Sockets Layer (SSL) in Transport Layer Security (TLS). Le-ta zagotavljata varne povezave in varnost pri prenosu gesel. Podpira vsa nujna stališča porazdeljene varnosti, vključno s porazdeljeno, skupno in mrežno avtentikacijo, porazdeljenim zaupanjem (angl. *distributed trust*) in

usmerjanjem pregleda, ki temelji na kontroli dostopa. Vse to je temelj za varno, porazdeljeno storitev.

- *Administracija*

  Izziv upravljanja v porazdeljenem okolju je skupno upravljanje strežnikov kot alternativa individualnemu. Modul CA Directory poenostavlja skupno upravljanje sistemskega imenika preko naslednjih značilnosti:

  - Globalna konfiguracija – ker imajo vsi strežniki isto konfiguracijo, je spremembe potrebno narediti samo enkrat. S tem smo tudi odstranili možnost napake pri konfiguraciji več strežnikov.
  - "Policy based control" – modul CA Directory dovoli definiranje konfiguracije po politiki dogovora, kar zelo poenostavi vzdrževanje, postavitev in revizijo.
  - Spletna administracija – modul CA Directory zagotavlja fleksibilno grafično spletno upravljani portal Dxmanager, ki ponuja grafično ponazoritev konfiguracije, statusa in nadzorovanja celotnega sistema.
  - Dinamična konfiguracija – večina operativnih nastavitev in vzdrževalnih korakov se lahko opravi med delovanjem modula CA Directory. To vključuje spremembe sheme, varnostne in administracijske kontrole kot so spletno nastavljanje in varnostno kopiranje (angl. *backup*).
  - Razsežna instrumentacija – CA Directory ima veliko lastnosti za omogočanje poročanja in nadzornih programov. Ob ostalih možnostih vsebuje tudi skupni čas delovanja dostopnosti statistike in dogajanja preko SNMP.

- *UNIX avtentikacija in "Pluggable authentication module" (PAM):*

  V velikih UNIX okoljih je individualno upravljanje z uporabniškimi računi dokaj težavno in precej drago. Z uporabo PAM-LDAP, CA Directory lahko integrira avtentikacijo vseh UNIX strojev v hrbtenico imenika. S centraliziranim upravljanjem so vsi računi in gesla shranjeni v imeniku, namesto na vsakem UNIX stroju posebej, so UNIX oskrbovanje, upravljanje in revizija zelo olajšani in poenostavljeni. LDAP V3 kontrola je dodana v Bind komponento UNIX, kar omogoča uporabo LDAP gesel na UNIX strojih.

- *Izboljšana podpora aplikacijam:*

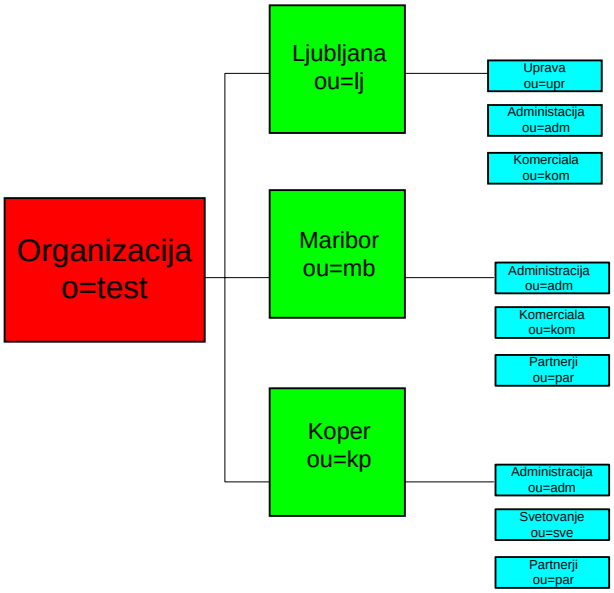
  Enotni atributi so pomembni za oskrbo aplikacije, kot so e-poštni naslovi, ključi in uporabniško ime, ki zahtevajo določene globalno enotne atribute. Tehnika znana tudi kot skupni atributi se izogiba shranjevanju iste vrednosti v več vnosnih enot, temveč shrani eno informacijo le enkrat, na ponavljajočih se lokacijah pa shranjuje kazalce na prvotno lokacijo.

3.3.2 Standardna arhitektura

Standardna CA Directory arhitektura je sledeča:

- LDAP V3.

- X.500 – za porazdeljenost in replikacijo - dovoljuje gradnjo poljubno velikega sistemskega imenika.
- Upravljanje (angl. *management*) - protokoli SNMP, CMIP, Telnet omogočajo poenostavljeno integracijo v celovito upravljanje sitema.
- Spletne storitve (angl. *web services*) - napredna UDDI in DSML sta sposobna podpirati številne aplikacije spletnih storitev.
- Shema LDAP – podpira vse glavne sheme in specifične prilagoditve (primer slika 7).



- **Slika 7. Shema LDAP.**

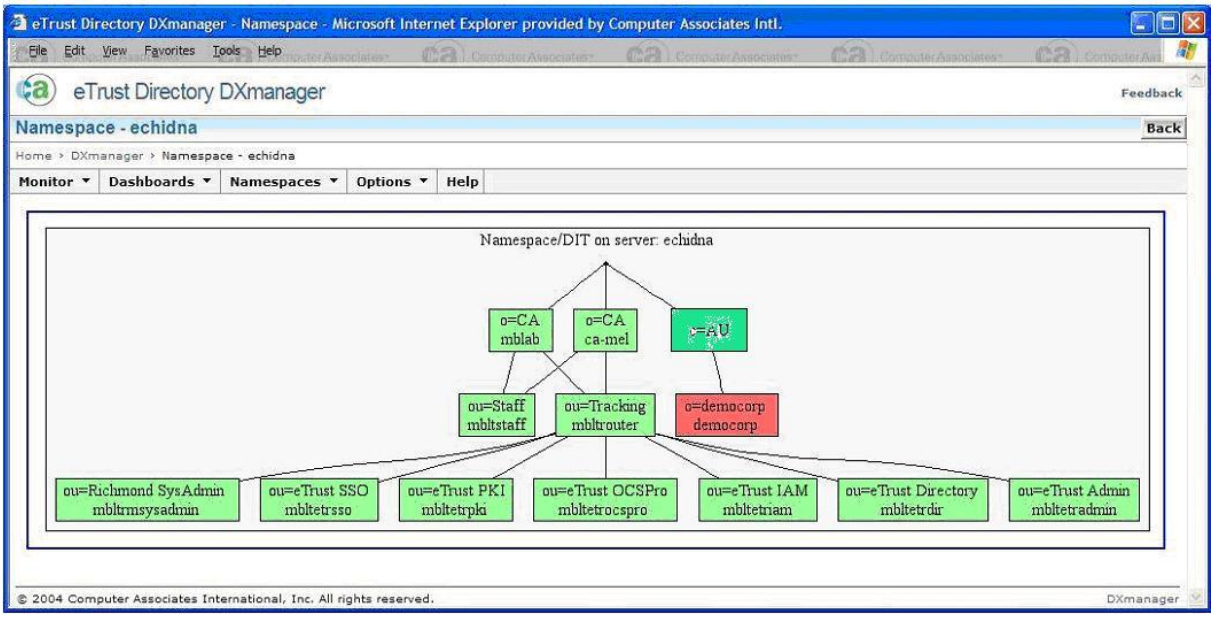
3.3.3 Komponente

Modul CA Directory je sestavljen iz nabora medsebojno povezanih komponent. V našem primeru smo se največ ukvarjali z naslednjimi [4]:

Dxserver je visoko zmogljivi LDAP/X.500 imeniški strežnik. Kot temeljna logična komponenta skrbi za vse LDAP operacije.

Dxmanager je centralni, spletno upravljalni grafični vmesnik, ki omogoča spremljanje, kontrolo in konfiguracijo (slika 8):

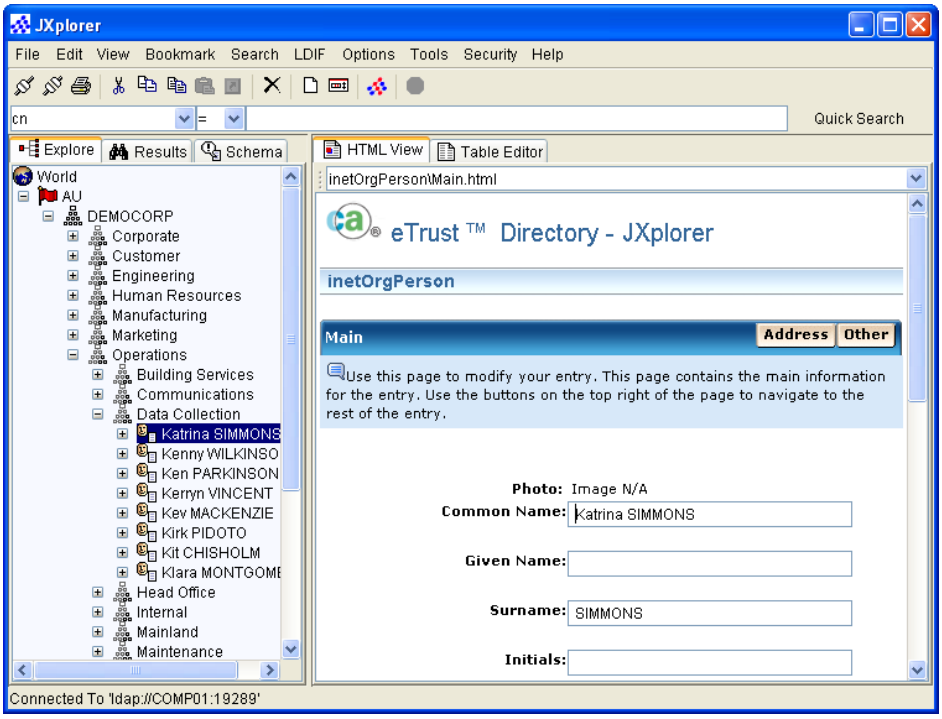
- "Monitoring" - modul Dxmanager omogoča spremljanje stanja sistemskega imenika in njegovih komponent v realnem času. Vsebuje grafe operacij, replikacijske vrste in statistiko nalaganja predpomnilnika.
- "Reporting" – modul Dxmanager omogoča frekvenčni histogram ažuriranja in iskanja za vsako vejo imenskega prostora. To omogoča prikaz poročil in načrtovanje dodajanja zmogljivosti.
- "Visualisation" – modul Dxmanager zagotavlja kaskadno vizualizacijo (angl. *drill-down*) statusnih map, gostiteljskih skupin, imenskih prostorov in povezav, omogoča hitro identifikacijo potencialnega ozkega grla ali drugih problemov.
- "Configuration" – modul Dxmanager lahko poroča o konfiguraciji, neprekinjenem delovanju in verziji produkta, kar pomaga pospešiti revizijo in diagnozo.



- **Slika 8. Vmesnik Dxmanager.**

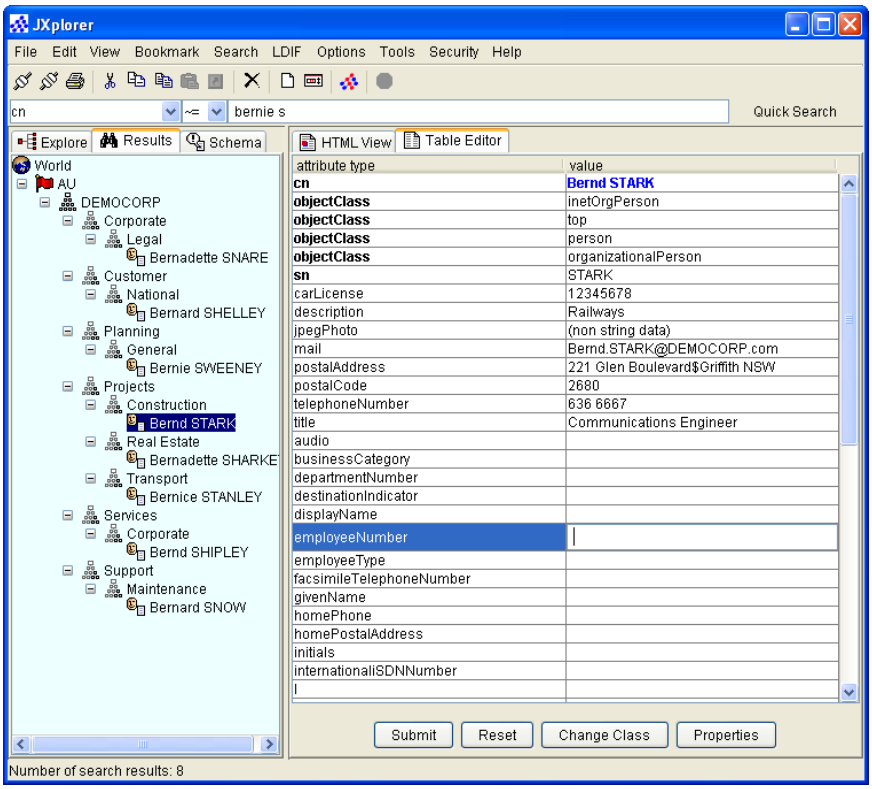
Dxtool je prilagodljiva množica orodij za upravljanje s podatki, atributi in shemo. Gre za skupino ukazno vrstičnih orodij za upravljanje s parametri delovanja sistemskih funkcij CA Directory.

Jxplorer je grafični, javanski preglednik in urejevalnik vsebine imenika LDAP. Na sliki 9 vidimo osnovni vmesnik, in sicer uporabniški imenik, v kateremu urejamo podatke o skupinah in uporabnikih.



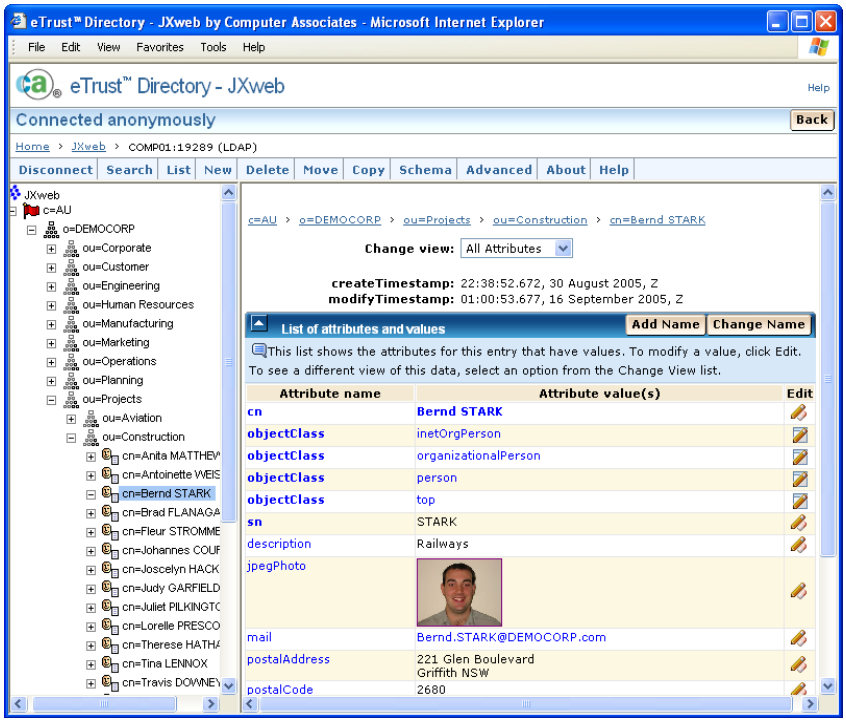
- **Slika 9. Jxplorer imenik.**

Na sliki 10 vidimo Jxplorer urejevalnik, v katerem lahko spreminjamo in urejamo vse ostale informacije o uporabniku, kot so naslov, e-pošta in telefon.

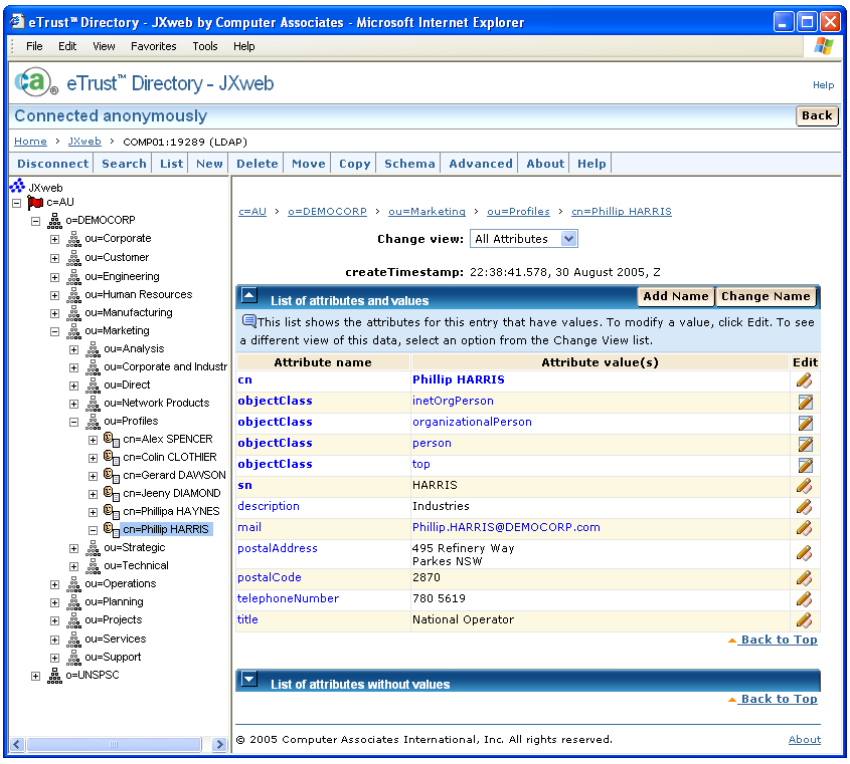


- **Slika 10. Jxplorer urejevalnik.**

Jxweb je grafični, spletni LDAP imenik preglednik in editor. Na slikah 11 in 12 vidimo osnovni vmesnik, v katerem lahko spreminjamo atribute in vrednosti določenih uporabnikov. Vsebuje večino funkcionalnosti Jxplorer vmesnika, uporablja pa se pretežno za oddaljeno administracijo.



- **Slika 11. Jxweb imenik.**



- **Slika 12. Jxweb urejevalnik.**

4 Implementacija sistema identitet

Diplomska naloga temelji na zoženem obsegu dejanskega projekta uvedbe sistema za upravljanje z identitetami in pristopi izpeljanega v večji organizaciji iz finančnega sektorja. Pri tem je bilo težišče na področju upravljanja z identitetami, in sicer uvajanja avtomatizacije v do sedaj ročno izvajane procese.

4.1 Pregled rešitve

Projekti implementacije rešitev za upravljanje z identitetami so specifični po kompleksnosti in številu tehnologij in procesov, s katerimi se povezujejo. Iz tega razloga se projektom vedno pristopa fazno. Izbrana rešitev temelji na posnetku stanja, na podlagi katerega je določena trenutna stopnja organizacijske zrelosti in pripravljenosti na upravljanje z identitetami. Ker se s trenutne stopnje lahko preide na več različnih naslednjih stopenj, so poslovne zahteve in operativni dejavniki služili kot smernice za precizno izvedbo stanja, ki bo rezultat tega projekta.

K sami implementaciji se je pristopilo takrat, ko so bile vse zahteve opredeljene po težavnosti, tveganjih in prednostih, ki jih bodo ustvarile. Rešitev predstavlja množico tehničnih sprememb s ciljem doseganja zahtevanih izboljšav. Z implementacijo spodnjih sprememb/izboljšav bo sistem dosegel večjo raven uspešnosti upravljanja z identitetami v IT:

- Avtomatična oskrba identitet

Zaloga identitet je postavljena in vzdrževana. Avtomatizirane operacije upravljanja računov, kot so dodajanje, spreminjanje in brisanje sedaj izvršuje sistem. Operacije se lahko avtomatično odvijajo preko več uporabniških računov. Te so lahko: potek dela, delegirana administracija, kadrovske funkcije ali posredne dejavnosti skrbnika varnosti.

- Avtomatizacija delovnega poteka

Delovni tok je definiran tako, da omogoči zahtevam za upravljanje identitet, da se inicializirajo, pregledajo in odobrijo. Delovni tok omogoča naslednje procese:

  - zaposlitev/prekinitev,
  - zahteva uporabniškega dostopa,
  - pregled računov,
  - pregled aplikacij,
  - definiranje politike in vzdrževanje.

Zahteve se lahko izvršijo s strani sistema za upravljanje identitet, preko avtomatične oskrbe računov ali s pomočjo drugih uporabnikov zunaj sistema.

- Delegirana uporabniška administracija

Poslovnega skrbnika lahko določimo kot delegiranega skrbnika za dodajanje, brisanje in spreminjanje uporabnika. Delegirani administratorji lahko uporabijo spremembe ali inicializirajo zahtevo za delovni tok. Skrbniki strank in partnerjev lahko dobijo pravice kot delegirani administratorji in lahko dodajajo in brišejo zunanje uporabnike (izvajalce, partnerje, kupce). Avtorizirani zunanji uporabniki lahko delujejo kot delegirani skrbniki za uporabnike in sisteme.

- Generiranje poročila uporabniškega računa

Poročila o uporabniških računih so lahko avtomatično generirana in pregled uporabniških računov je lahko tudi del delovnega toka.

- Korelacija z avtoritativnimi viri

Osnovni poslovni sistem za upravljanje s kadri ponavadi uporabljamo kot avtoritativni vir za spremembe na uporabniških računih. Odstranitev uporabnika v kadrovskem sistemu lahko uporabimo za brisanje uporabniškega računa.

- Politika upravljanja identitet in upravljanje procesov

Delovni tokovi so določeni tako, da omogočijo politiko upravljanja identitet in vzdrževanje procesov, lahko pa tudi podprejo dodajanje procesov novi aplikaciji ali strežniku.

4.2 Predstavitev procesov v rešitvi

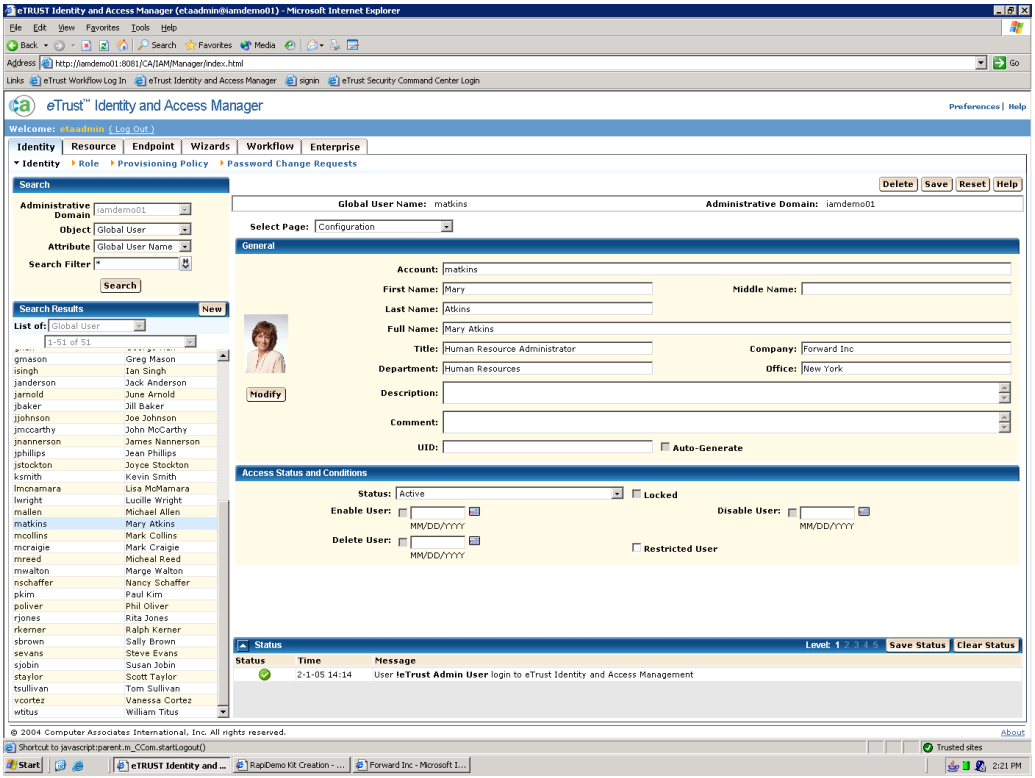
Naslednji procesi so definirani tako, da izboljšajo obstoječe delovanje z avtomatizacijo in usklajevanjem delovnega toka:

- Novi zaposleni
- Novi zunanji sodelavec
- Revizija varnosti uporabniškega računa
- Zahteva po uporabniškem dostopu
- Odstranitev uporabnika
- Novi strežnik/aplikacija
- Definiranje politik
- Ponastavitev uporabniškega gesla

Kot razširitev v upravljanju identitet sta uvedena dva procesa:

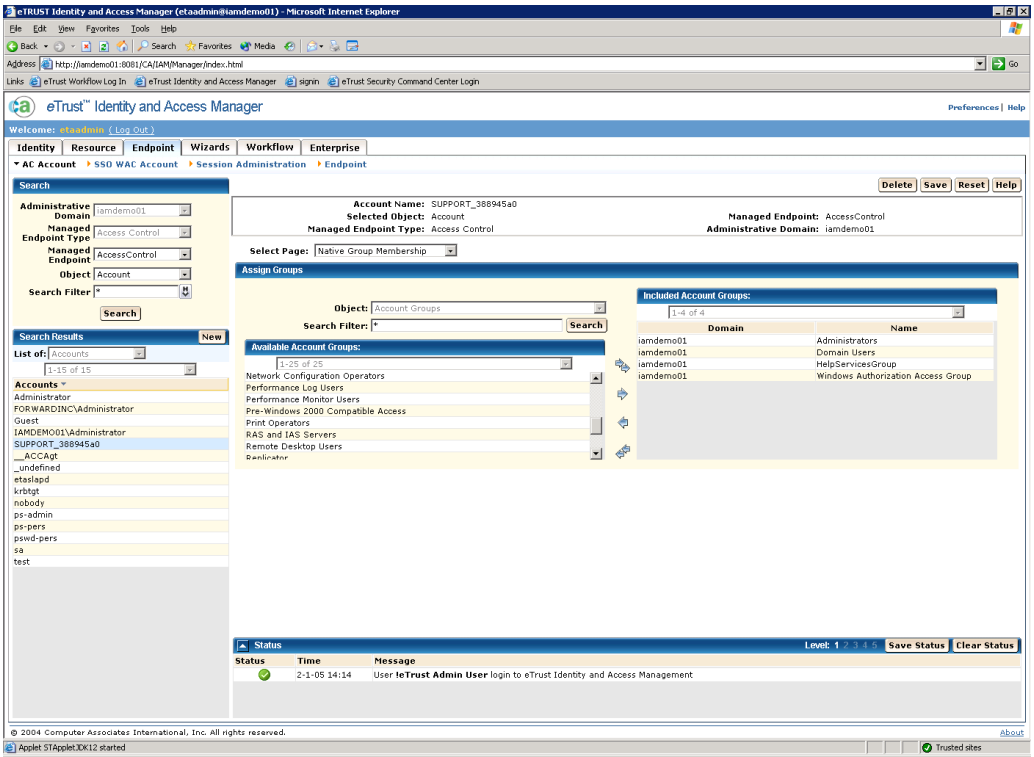
- Integracija upravljanja identitet strežnika ali aplikacije.
- Definirana politika in standardi za upravljanje identitet.

V nadaljevanju bomo predstavili osnovne vmesnike za upravljanje uporabnikov, upravljanje vlog in dodeljevanje pravic. Na sliki 13 vidimo prvi korak procesa dodajanja novega uporabnika, kjer ustvarjamo identiteto ter ji dodeljujemo osnovne podatke in določamo časovno obdobje, v katerem imajo identiteta in nanjo vezane pravice aktiven status. V primeru odhoda osebe iz organizacije, se identiteta osebe deaktivira za obdobje 2 let. Po preteku tega obdobja se podatki trajno brišejo.



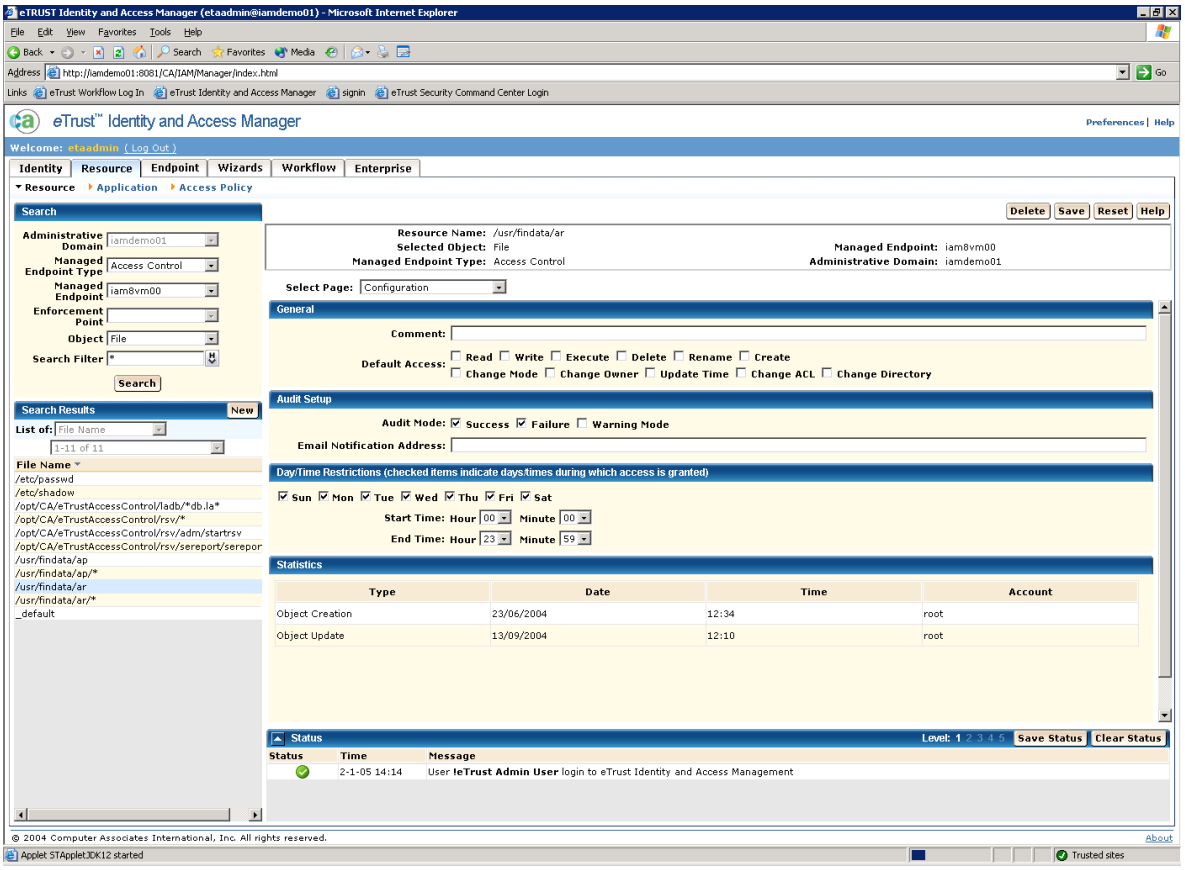
- **Slika 13. Upravljanje uporabnikov.**

Na sliki 14 vidimo naslednji korak, v katerem osebo (identiteto) vključimo v določene skupine. S tem korakom se začne delovni tok za pridobivanje pravic, vezanih na te skupine.



- **Slika 14. Vmesnik za upravljanje vlog.**

Na sliki 15 vidimo korak procesa, v katerem skupinam dodeljujemo določene pristopne pravice, skupaj z vsemi naprednimi parametri.

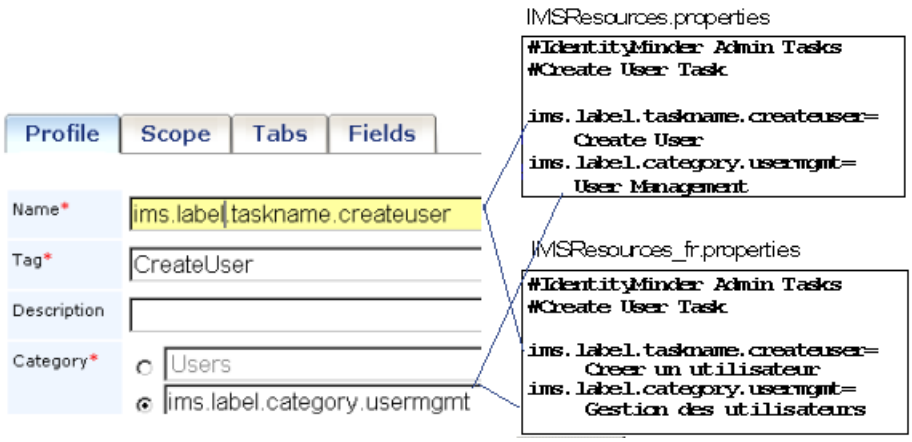


- **Slika 15. Vmesnik za dodeljevanje pravic.**

4.2.1 Novi zaposleni

Dodajanje uporabnika v kadrovski sistem povzroča dodaten delovni potek, ki skrbi za uporabniško oskrbo. IT operativa ni več odgovorna za postavitev in vzdrževanje uporabnikov za infrastrukturne sisteme (LAN, e-pošta). Skrbnik varnosti tukaj prevzame odgovornost za to vlogo. Sistem za upravljanje identitet se uporablja za avtomatizacijo postavljanja računov za infrastrukturne sisteme, korporativni direktorij identitet in za vse aplikacije, ki uporabljajo ta direktorij. Za ostale aplikacije skrbniki aplikacij še vedno upravljajo račune in dovoljenja, lahko pa se sklicujejo na zunanji avtoritativni direktorij. Za zahtevane spremembe, ki niso direktno del informacijske tehnologije delovni tok sproži zahtevek za inventarskega skrbnika. Na sliki 16 vidimo administratorsko okno za dodajanje novega uporabnika.

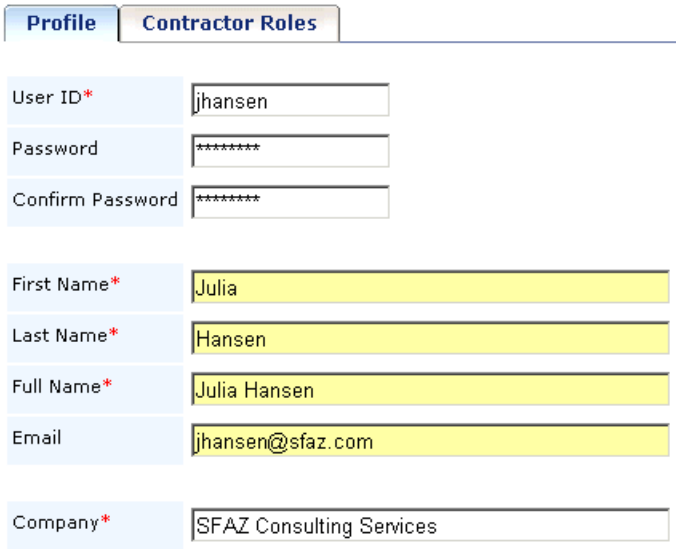
•



- **Slika 16. Dodajanje novega uporabnika in spremembe atributov v ozadju.**

4.2.2 Novi zunanji sodelavec

Proces se začne z delegirano zahtevo partnerja, kupca, izvajalca v organizaciji. Politika varnosti organizacije določa, katere zunanje organizacije lahko dostopijo in kateri tip dostopa imajo. Skrbnik strank in partnerjev mora odobriti zahteve po zunanjem dostopu. Postavitev uporabniškega računa je avtomatična, vključno s pošiljanjem zahtev za odobritev določenih korakov pristojnim osebam. Na sliki 17 vidimo osnovno okno za vpis novega zunanjega sodelavca.



- **Slika 17. Vnos osnovnih atributov zunanjega uporabnika.**

4.2.3 Revizija varnosti uporabniškega računa

Slika 18 kaže vmesnik za določanje omejitev v povezavi s politiko razdeljevanja dolžnosti (angl. *segregation of duties*), kot ene od osnovnih revizijskih zahtev.

- **Slika 18. Preverjanje politike za razdeljevanje dolžnosti.**

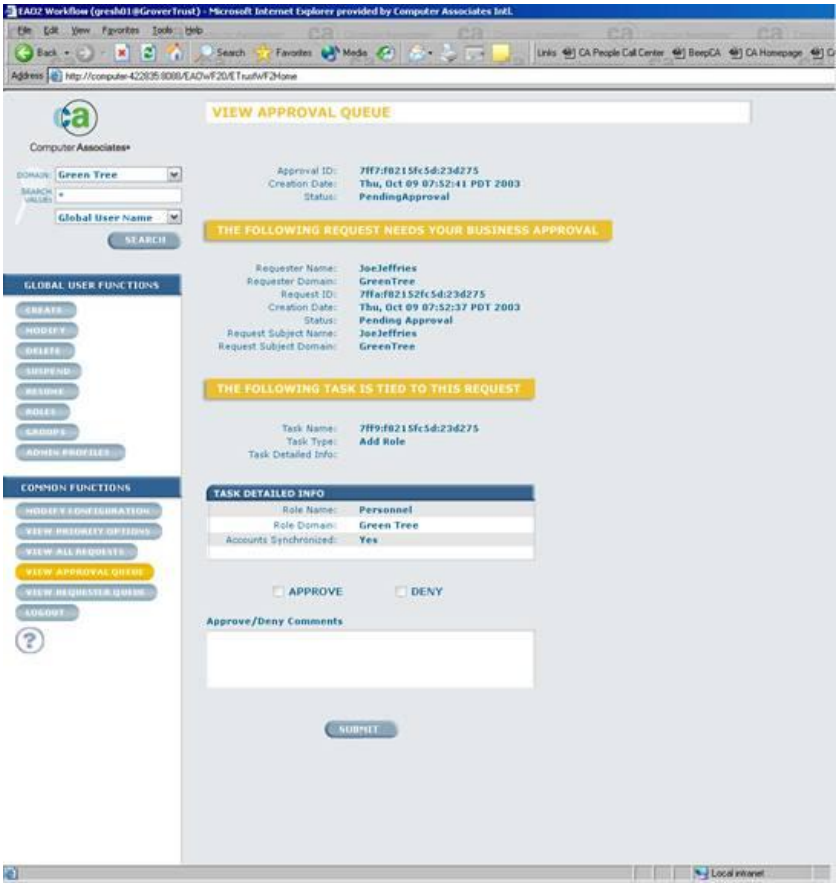
Proces revizije varnosti uporabniškega računa se začne z avtomatično sinhronizacijo med avtoritativnimi viri uporabnikov in uporabniškimi računi v infrastrukturnem sistemu, korporativnem imeniku identitet in aplikacij. Če so slučajno opaženi mrtvi (angl. *Ghost user*) računi, se aktivira servisna zahteva za shranjevanje podatkov in se po potrebi račun avtomatično izbriše. Poročila uporabniških računov so avtomatično predložena s strani sistema za upravljanje identitet in so dostopna za notranjo ali zunanjo revizijo. Pregled poročil uporabniških dostopov za natančno določene pravice je potrebno izvesti ročno. Vsaka sprememba poročila je avtomatično procesirana v sistemu za upravljanje identitet in pripravljena za pregled, ko ga zahteva notranja ali zunanja revizija. Pregled sprememb pravilnosti je potrebno narediti ročno.

4.2.4 Zahteva po uporabniškem dostopu

Zahteva uporabnika za dostop je rešena tako, da končni uporabnik preko lastnega vmesnika inicializira proces za dodatni dostop. Preden se akcija izvede mora biti odobrena zahteva z višje ravni, odvisna pa je od zahteve za dostop, ki se nanaša na naslednje primere:

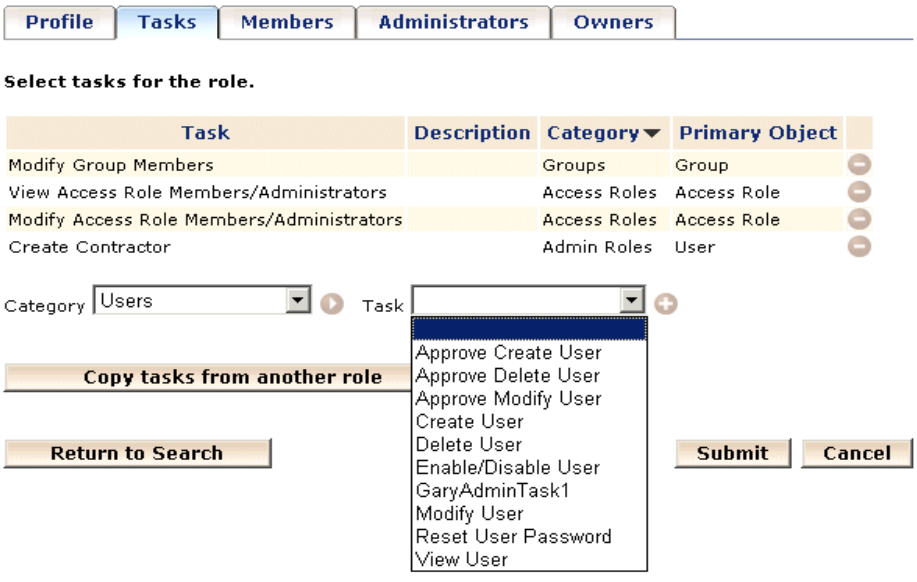
- Zaposleni potrebuje odobritev zahteve od skrbnika.
- Zunanji uporabnik potrebuje dovoljenje za dostop od skrbnika strank in partnerjev.
- Za dostop do poslovnih aplikacij potrebuje dovoljenje skrbnika aplikacije.
- Ostala dovoljenja so lahko del politike.

Na sliki 19 vidimo prikaz vmesnika, v katerem skrbnik lahko odobri ali zavrne avtomatično generirano zahtevo za odobritev dodeljevanja aplikacijske vloge uporabniku.



- **Slika 19. Prikaz vmesnika za odobritev dodeljevanja vloge uporabniku.**

Servisne zahteve za spremembo dostopa do infrastrukture izvršuje skrbnik varnosti s koraki, ki so avtomatizirani s sistemom upravljanja identitet. Servisne zahteve za spremembo dostopa poslovne aplikacije izvršuje skrbnik aplikacij. Na sliki 20 vidimo vmesnik za dodeljevanje administrativnih nalog uporabniku.



- **Slika 20. Dodeljevanje administrativnih nalog.**

4.2.5 Odstranitev uporabnika

Proces odstranitve uporabnika se izvede, ko je zaposleni odstranjen iz kadrovskega sistema, odstranitev zunanjega uporabnika pa zahteva delegirani administrator. Skrbnik strank in partnerjev odstrani uporabnika iz avtoritativnega seznama zunanjega uporabnika. Rezultat je viden v reviziji varnosti uporabniškega računa. To nato sproži servisno zahtevo za shranjevanje podatkov in brisanje računa.

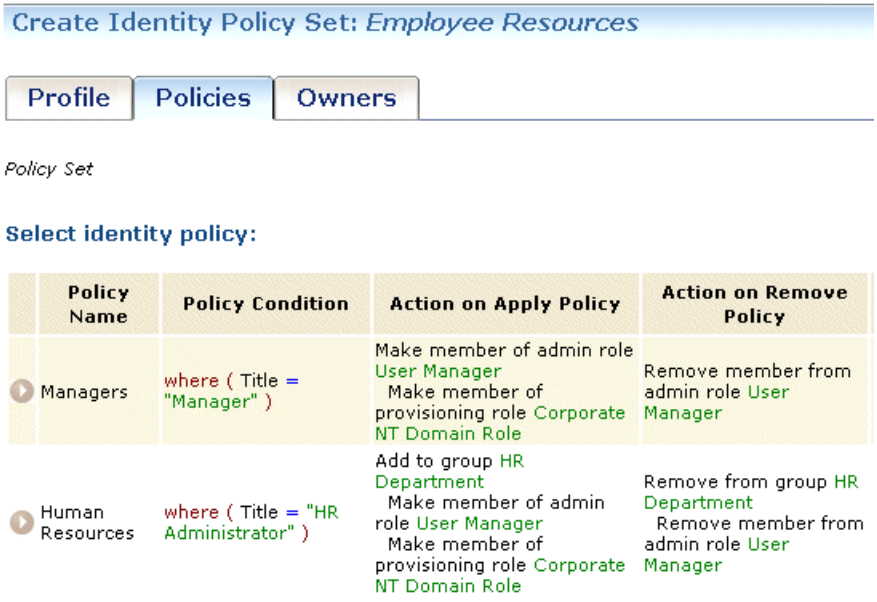
4.2.6 Novi strežnik/aplikacija

Osnovni projektni koraki od začetne zahteve za razvoj nove aplikacije do samega prehoda v produkcijsko okolje ostajajo enaki kot pred uvedbo rešitve. CA Identity Manager sedaj skrbi za dajanje odobritev za pristope projektnemu osebju. Po integraciji nove aplikacije z orodjem CA Identity Manager, se vse operacije upravljanja z njenimi uporabniki izvajajo in nadzorujejo v skladu z definiranimi politikami.

4.2.7 Definiranje politik

Politike se definirajo in predpisujejo v orodju Identity Manager v skladu s pravicami skrbnikov. Ključna razlika je v centralnem, avtomatiziranem izvajanju politik, ki skrbnikom posameznih aplikacij ne omogoča lastnoročnega spreminjanja globalnih pravil.

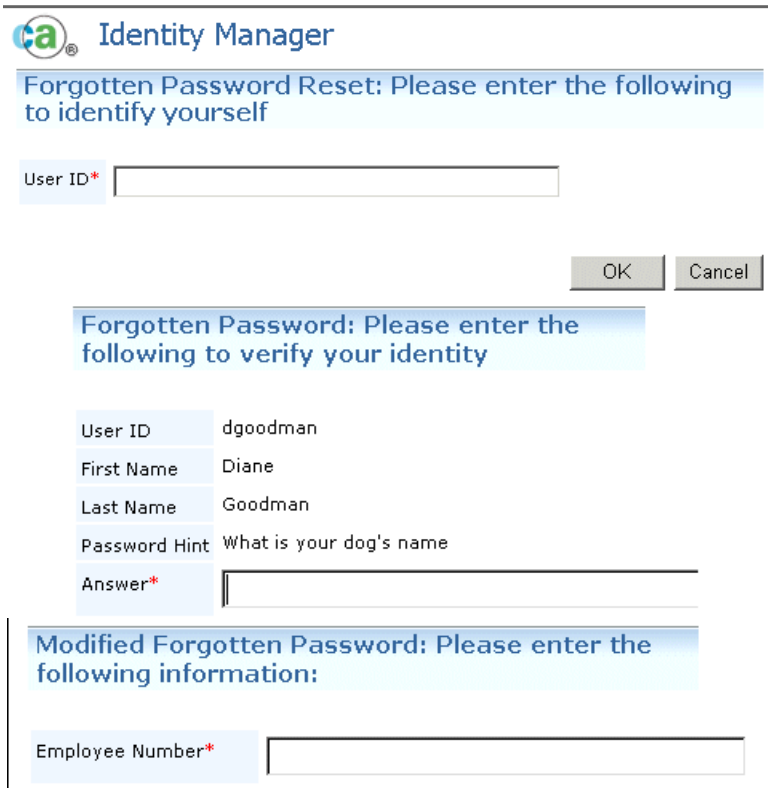
Slika 21 ponazarja upravljanje s politiko pridruževanja vlog po kriteriju delovnega mesta.



- **Slika 21. Upravljanje s politiko dodeljevanja organizacijskih vlog.**

4.2.8 Ponastavitev uporabniškega gesla

Za ponastavitev gesla na sistemih, ki jih upravlja CA Identity Manager, se uporabnik avtenticira na podlagi svojih osebnih informacij. Po uspešni avtentikaciji sistem za upravljanje z gesli avtomatično izvršuje spremembo in spreminja geslo v sistemu. Slika 22 kaže proces avtentikacije uporabnika za potrebe ponastavitve pozabljenega gesla.



- **Slika 22. Avtentikacija za ponastavitev pozabljenega gesla.**

4.3 Vrste entitet v organizaciji

V naslednji tabeli so prikazane različne vrste entitet v organizaciji, ki smo jih srečali v našem primeru. Opisane so vloge, njihova trenutna uporaba in pričakovana uporaba po implemetaciji rešitve.

Vloga	Opis	Trenutna uporaba	Pričakovana uporaba
Predstojnik oddelka za informacijsko varnost	Predstojnik oddelka za informacijsko varnost	Odgovoren je za varnostno politiko	Lahko uporablja sistem za definiranje procesov in administrativno lastništvo.
Skrbnik za varnost informacijskih sistemov	Administracija varnosti	Dodaja, briše in spreminja uporabniške račune in jih pregleduje. Upravlja s spreminjanjem imenskega prostora.	Uporablja spletno administracijo in vmesnik poteka dela za upravljanje identitet.
Zaposleni	Končni uporabnik, ki zahteva dostop do IT sistemov, poslovnih aplikacij in virov, ki niso direktno informacijske tehnologije.	Zaposleni pošlje zahtevo za upravljanje identitet preko svojega skrbnika ali preko telefona/fax-a.	Uporablja spletno samopostrežno administracijo in vmesnik poteka dela za upravljanje identitet.

Poslovni skrbnik	Skrbnik zaposlenih	Vnaša ročno zahtevo za dostop uporabnika.	Poslovni skrbnik lahko izvrši delegirano administracijo ali odobri zahtevo delovnega toka za njegovega uporabnika.
Človeški viri Kadrovska služba	Kadrovska služba je odgovorna za skrb za zaposlene pri zaposlitvi ali odhodu iz organizacije.	Upravlja nove zaposlitve in odpuščanja preko kadrovske poslovne aplikacije.	Poslovni skrbnik lahko izvrši delegirano administracijo ali dovoli zahtevo delovnega toka za njegovega uporabnika.
Skrbnik aplikacij	Lastnik poslovnih aplikacij.	Dovoli ročno zahtevan dostop do poslovnih aplikacij.	Sprejema obvestilo delovnega toka zahtev uporabniškega dostopa in potrditve dokončnega stanja.
Inventarni skrbnik	Upravljanje virov, ki niso direktno informacijske tehnologije.	Omogoča ročno zahtevan dostop do virov, ki niso direktno informacijske tehnologije.	Sprejema notifikacijo delovnega toka zahtev uporabniškega dostopa in potrditve dokončnega stanja.
Zunanji sodelavec	Uporabnik, ki potrebuje račun v sistemu in ni zaposlen v podjetju	Računi se definirajo po zahtevi direktno ali preko skrbnika strank in partnerjev.	Zunanji uporabniki imajo samopostrežno administracijo in možnost ponastavljanja, če je prej dovoljeno.
Skrbnik strank in partnerjev	Skrbnik strank in partnerjev za kupce, partnerje in izvajalce	Skrbnik strank in partnerjev ročno pošilja zahteve za dostop do virov, ki niso direktno informacijske tehnologije.	Poslovni skrbnik lahko izvrši delegirano administracijo, ali lahko dovoli zahtevo delovnega toka za njegovega uporabnika.
Skrbnik za razvoj	Razvija in dobavlja aplikacije	Preden začne z razvojem, skrbnik za razvoj dokumentira upravljanje varnosti in uporabniško upravljanje za novo aplikacijo.	Kot del razvoja nove aplikacije skrbnik za razvoj integrira standarde upravljanja identitet in preverja skladnost.
IT skrbnik	Izvaja ročne naloge	Po ročni zahtevi priskrbi prenosne računalnike za nove zaposlene.	Sprejel bo avtomatično obvestilo o zahtevi za prenosnim računalnikom.

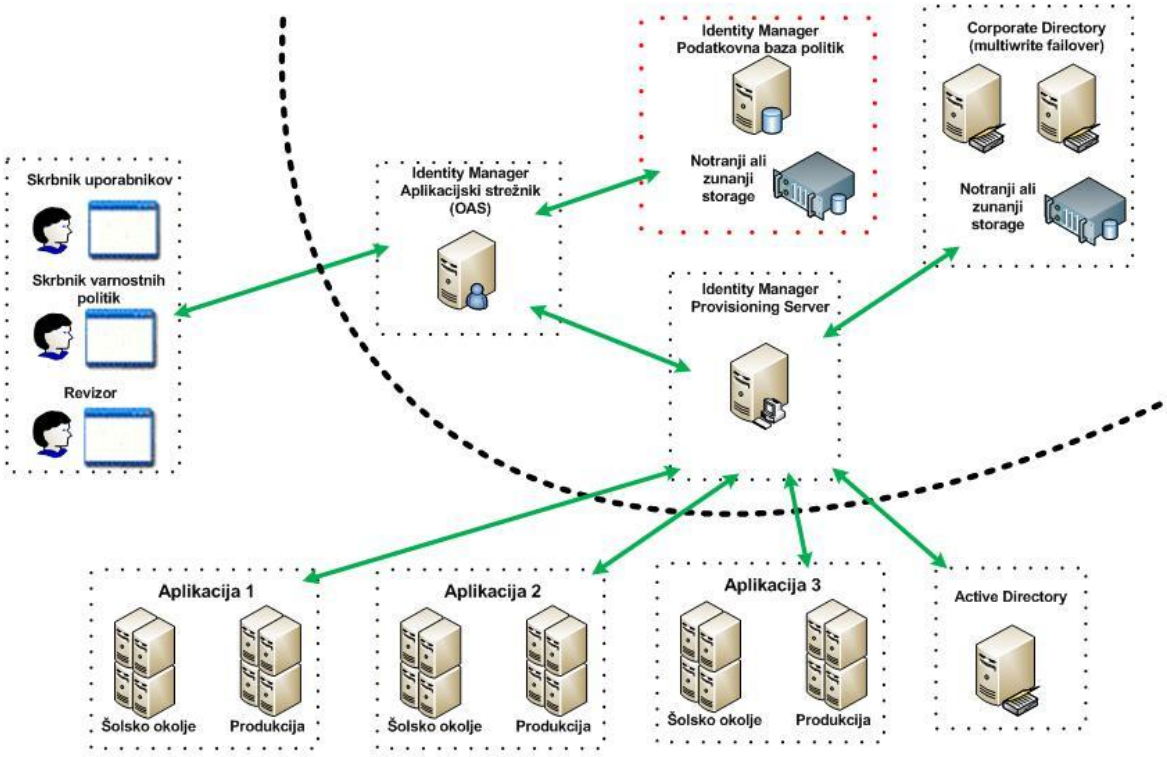
-

Tukaj bom naštel nekaj medsebojnih vplivov v procesu reševanja in izboljšave sistema identitet:

- Politike, tehnične standarde, lastnike procesov določa predstojnik oddelka za informacijsko varnost.
- Predstojnik oddelka za informacijsko varnost ocenjuje, kako skrbnik varnosti skrbi za upravljanje varnosti in periodične preglede uporabniških računov.
- Tehnične standarde, katere določi predstojnik oddelka za informacijsko varnost, morajo upoštevati tudi razvijalci.
- Kadrovska služba skrbi za postopke nove zaposlitve in odpuščanja.
- Aplikativni in inventarski skrbniki dobijo končna obvestila zahtev za omogočanje, spreminjanje in brisanje dostopov uporabnika.
- Končni uporabniki in uporabniki z delegiranim upravljanjem bodo imeli možnost upravljanja z računi, vključujoč upravljanje z gesli.

4.4 Arhitektura rešitve

Na sliki 23 vidimo planirano arhitekturo rešitve za našo organizacijo. Vidimo medsebojno povezanost določenih aplikacij (aplikacija 1,2,3) ter aktivnega imenika s centralnim sistemom CA Identity Manager, ter njegovo zvezo s procesi in komunikacijo v ozadju (imenik, baza politik) ter aplikacijskim strežnikom, ki povezuje končne uporabnike (skrbnike, revizorje) s samim sistemom.



- **Slika 23. Arhitektura rešitve.**

4.4.1 Arhitekturni koncepti

Planirana arhitektura uporablja navidezni imenik, upravljanje z identitetami in podporne module. Naša rešitev vključuje naslednje glavne arhitekturne komponente:

- *Navidezni imenik* povezuje človeške identitete (globalne uporabnike) z uporabniškimi računi (urejeni imenski prostori) preko definirane preslikave replikativnega navideznega imenika.

- *Oskrba strežnika,* kjer replikativni strežnik prilagodi upravljalne operacije multipliciranim imenskim prostorom skozi množico specifičnih komunikacijskih protokolov (dostopnih kot opcija za vsak imenski prostor).

- *Replikacija in razdeljevanje obremenitve* (angl. *load-balancing*), kjer vgrajeno usmerjanje na aplikativni plasti podpira večkratne navidezne direktorije, kot tudi večkratno oskrbo strežnikov, pripravljenih za specifično okolje.

- *Porazdeljeno upravljanje odjemalcev,* kjer je veliki del odjemalcev za dodajanje, brisanje in ažuriranje identitet in uporabniških računov. Uporabljajo se brskalnik za samopostrežno administracijo, Win32 manager, CLI, LDAP, Java, LDIF import/export, SPML.

- *Podporni moduli*, ki vsebujejo mehanizem delovnega toka, sinhronizacijo gesla, poročanje in zajemanje avtoritativnih virov.

4.4.2 Administrativni koncepti

Planirana arhitektura podpira naslednji administrativni model z upravljalskimi operacijami:

Globalno uporabniško upravljanje, kjer globalne uporabnike lahko kreiramo, ažuriramo, brišemo, dodajamo skupinam, pridružujemo imenskim prostorom, dovoljujemo možnost samopostrežne administracije ter sodelovanje v delovnem toku.

Direktno upravljanje računov, kjer se uporabniški računi, skupine in gesla v imenskem prostoru lahko definirajo, ažurirajo in brišejo preko Win 32 vmesnika ali brskalnika.

Indirektno upravljanje računov - za vse tiste imenske prostore, ki jih ne moremo upravljati na direkten način, pošiljamo obvestilo pristojnemu skrbniku, ki ažurira podatke uporabniškega računa. Skrbnik nato spremeni status zahtevka, zaradi neprekinjenega spremljanja delovnega toka.

Postavitev globalnih uporabnikov, kjer so globalni uporabniki lahko definirani medsebojno, ali običajno na podlagi odkritja in korelacije obstoječih imenskih prostorov ali kot rezultat iskanja podatkov kadrovskega sistema.

Domenska administracija, kjer struktura naslovnega prostora podpira modeliranje organizacije. To omogoča strukture enojnih naslovnih prostorov (angl. *single-domain*) ali

hierarhičnih več naslovnih prostorov (angl. *multi-domain*) za globalne uporabnike in druge objekte. Splošni objekti so lahko definirani na višjem nivoju hierarhije.

Politike so definirane tako, da predstavljajo običajne postavitve in privilegije, ki delijo več uporabnikov v določenem imenskem prostoru.

Administrativni profil, ki določa obseg objektov in operacij administracije ter se lahko pridružuje globalnim uporabnikom, ki izvršujejo administracijo.
Zunanja avtentikacija je varna avtentikacija na podlagi zunanje tehnologije (npr. biometrija, "token", PKI), ki omogoča dodatno preverjanje identitet.

Poročanje se izvršuje na navideznem imeniku prirejenem za želeni format.

4.4.3 Elementi rešitve

Elementi modulov CA Admin in CA Identity and Access Management, ki so uporabljeni v implementaciji načrtovane rešitve so [3]:

- *Elementi strežnika:*

"Provisioning Service sladp" je komponenta, ki sprejema zahtevo od odjemalca in ažurira imenski prostor, kjer je treba.

"Superagent Service" je komponenta, ki usmerja zahteve do imenskih prostorov preko množice opcij.

"Provisioning Service DXRouter" je komponenta, ki se uporablja za uravnoteženje bremena in nadomestnega načina delovanja z usmerjanjem zahtev med komponentami "Provisioning Service sladp".

"Administrative Directory DXServer" je komponenta, ki implementira navidezni imenik.

"Administrative Directory DXRouter" je komponenta, ki se uporablja za razdeljevanje obremenitve in kot nadomestni način delovanja z usmerjanjem zahtev med komponentami "CA Directory".

"Workflow Server" je strežnik, ki skrbi, da delovni tok deluje v spletnem vmesniku in preko "Universal Feed" opcije.

"Workflow Directory DXServer" je komponenta, ki uporablja strežnik delovnega toka za shranjevanje podatkov.

"Ingres" je zaloga podatkov, katero uporabljajo DXServer komponenta, napredni delovni tok in podatkovna baza poročil.

"Web Application Server" je spletni strežnik, ki dostopa do spletnih komponent odjemalca.

- *Elementi odjemalca:*

  - *Administrativne komponente*

"Admin Manager" je komponenta, ki skrbi za Windows grafični uporabniški vmesnik (angl. *Windows GUI*), kjer se izvršujejo administrativne naloge. Te naloge so: upravljanje uporabnikov, upravljanje skupin, upravljanje računov itd. Samo avtorizirani administratorji imajo dostop do GUI-ja in obsežne administrativne pravice so lahko dodeljene različnim administratorjem.
"Etautil" je komponenta, ki skrbi za vmesnik za ukazno vrstico in izvrševanje administrativnih operacij.

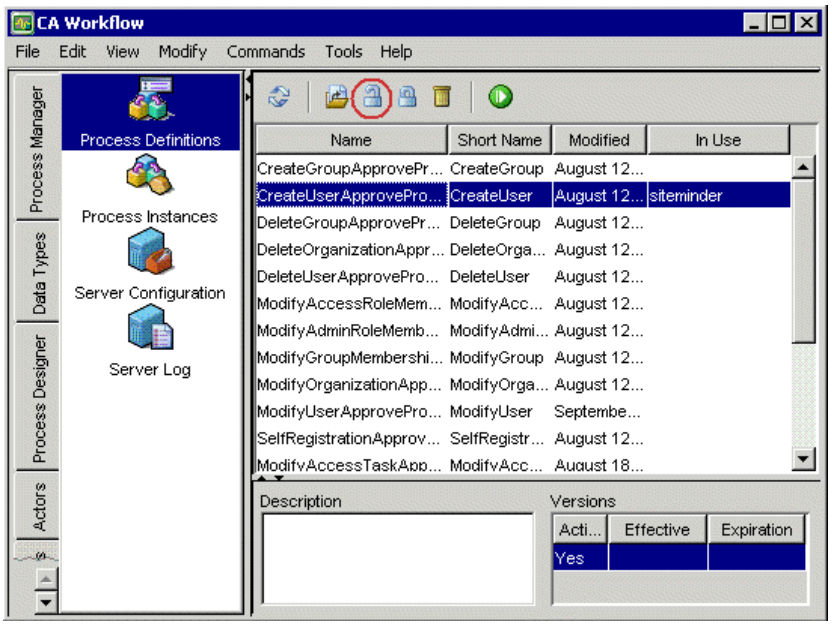
"IDE" komponenta omogoča definiranje naprednih procesov delovnega toka in konfiguracijo obstoječih procesov.

  - *Delegirane administrativne komponente*

"IA Manager" je komponenta, ki skrbi, da spletni vmesnik izvrši administrativne operacije za avtoriziranje administratorjev na podlagi njihovih vnaprej definiranih administratorskih profilov.

"Workflow Web Interface" je komponenta, ki skrbi za spletni vmesnik v katerem dovoljujemo uporabniške zahteve za dostop do aplikacij, ki so potrebne za njihovo delo. Zahteva mora biti odobrena s strani enega ali več avtoriziranih skrbnikov, preden je izvršena.

"Advanced Workflow Client" je komponenta, ki omogoča pregledovanje poslovne liste – dostopno preko modula IA Manager (slika 24).



- **Slika 24. Advanced Workflow Client.**

"Self Service" je komponenta, ki omogoča končnim uporabnikom, da se avtentificirajo, ponastavijo gesla in vložijo zahteve delovnega toka [1].

- *Komponente poročanja*

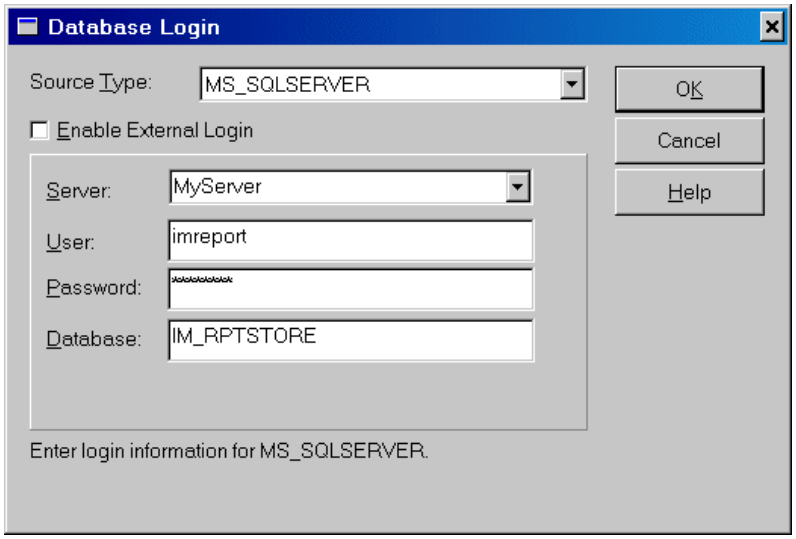
Na sliki 25 vidimo osnovno okno za prijavo v bazo poročil z naslednjimi komponentami:

"GUExtract" je komponenta, ki izloči globalne uporabnike v podatkovno bazo poročil.

"BatchExtract" je komponenta, ki izvleče objekte v podatkovno bazo poročil.

"Report Explorer" je komponenta, ki izvleče objekte, generira in pregleduje poročila.

"Caqr31ch" je komponenta, ki generira poročila iz podatkovne baze poročil.



- **Slika 25. Prijava v bazo poročil.**

- *Komponente vmesnika imenskega prostora* [3]:

"Universal Feed Option" je komponenta, ki sprejema spremembe zapisov zunanjega avtoritativnega vira in jih preoblikuje za predložitev v strežnik delovnega roka.

"Managed Options" – možnosti upravljanja.

"ADS Option" je komponenta, ki omogoča upravljanje uporabnikov in skupin v aktivnem imeniku.

"Windows Option" je komponenta, ki omogoča upravljanje uporabnikov in skupin v Windows sistemih.

"Windows agent" je komponenta, ki omogoča komunikacijo Windows Option z Windows strežnikom, uporabljajoč CA tehnologijo obvestil CAM/CAFT.

"UNIX ali Linux Option" je komponenta, ki omogoča upravljanje uporabnikov in skupin v UNIX ali Linux sistemih.

"UNIX ali Linux agent" je komponenta, ki omogoča komunikacijo od UNIX ali Linux Option do Unix ali Linux sistemov, uporabljajoč CA tehnologijo obvestil CAM/CAFT.

"ACF2 ali RACF Option" je komponenta, ki se povezuje z zunanjim varnostnim managerjem (angl. *External Security Manager ESM', CA-ACF2 or RACF*) z/OS LPAR, da dobi uporabniški ID in skupino ter njihov dostop do virov.

"Universal Provisioning Option" je komponenta, ki se lahko uporablja za povezovanje z aplikacijami, ki niso integrirane z modulom CA Admin. CA Admin kot univerzalna komponenta za oskrbo uporabnikov lahko pošilja elektronska sporočila aplikativnim administratorjem z navodili za uporabniško oskrbovanje (angl. *user provisioning)*.

4.5 Prikaz rešitve

4.5.1 Dokumentacija

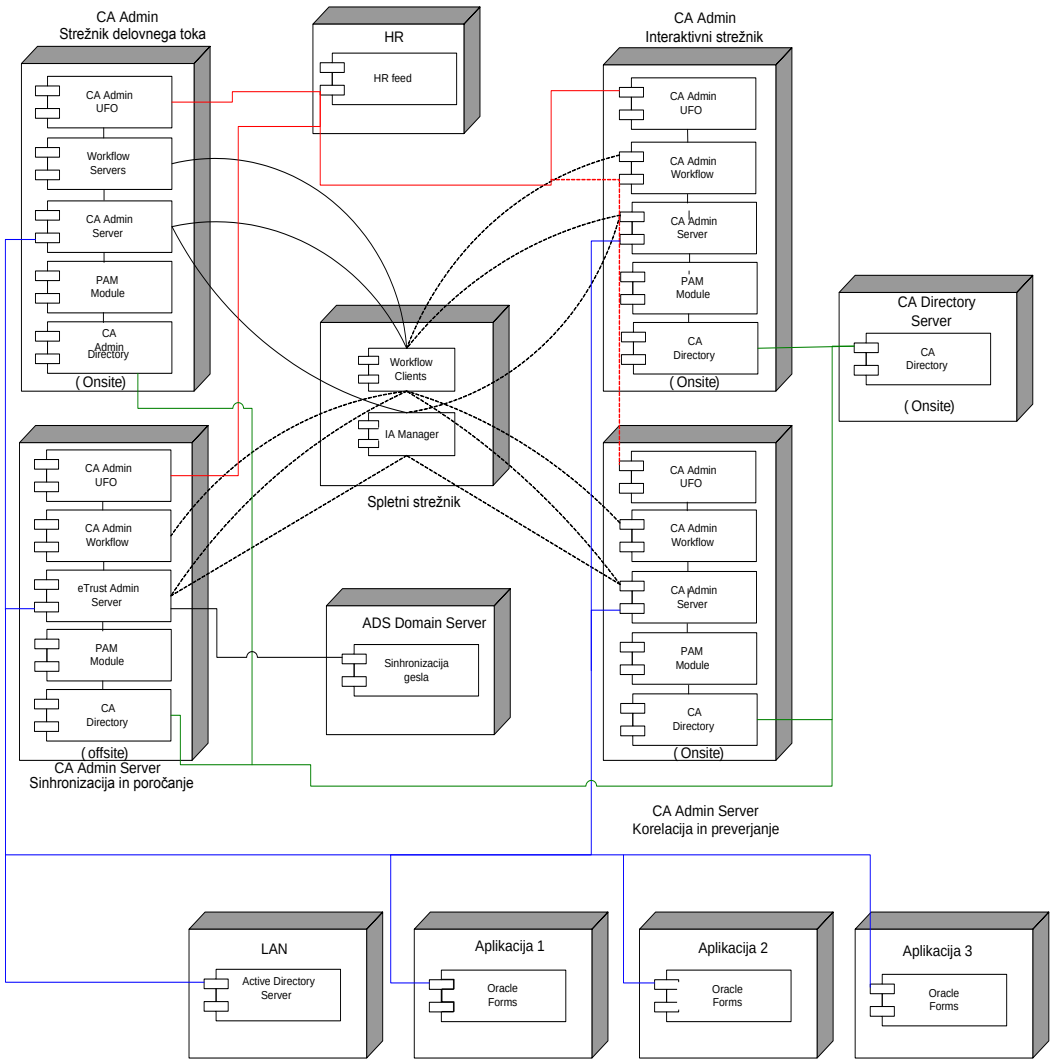
Vsaka končna rešitev uporablja vrsto spremljevalnih dokumentov, katerih vsak del je ključnega pomena za uspešno samostojno uporabo rešitve. Zaradi kompleksnosti in števila povezav različnih CA-IM gradnikov, kot so podatkovne baze, aplikacije, operativni sistemi, procesi, zaposleni, stranke in revizorji, predstavlja dobra dokumentacija temelj za nadgradnjo sistema. Glavni dokumenti so obrazloženi v spodnji tabeli:

Opis dela	Začetni dokument, ki točno določa dolžnosti naročnika in izvajalca – kaj bo dobavljeno, kateri sistemi bodo zajeti v projektu in v kakšni meri. To zagotavlja naročniku, da bo obseg projekta v skladu z njegovimi zahtevami in pričakovanji.
Pregled arhitekturne rešitve	Osnovni arhitekturni dokument, ki podrobno definira: • Poslovne zahteve • Zahteve po rešitvi • Kriterije za uspeh projekta • Organizacijski kontekst • Trenutno stanje • Želeno stanje, razdelano do podrobnosti v smislu konceptov in tehničnih zahtev • Akterje v projektu in organizaciji kot celoti in njihove interakcije • Scenarije uporabe in poskusov zlorabe rešitve (potek in pričakovani rezultati) za potrebe kasnejšega testiranja • Arhitekturo rešitve (grafični prikaz, opis vseh komponent) • Specifikacijo integracije z obstoječimi sistemi • Vpliv sprememb na poslovne procese • Vpliv sprememb na ljudi • Vpliv sprememb na tehnične komponente • Definiranje metrik kvalitetne rešitve (zanesljivost, dosegljivost in uporabnost) • Dobre prakse za uporabo in vzdrževanje • Plan testiranja • Projektni plan in komentar
Specifikacija arhitekture rešitve	Razširitev "Solution Architecture Overview" dokumenta. Pri manjših projektih ter pri zelo časovno omejenih projektih se uporablja le en od naslednjih dveh dokumentov - SAO ali SAS.
Projektni plan	Projektni plan razdelan do ravni posameznih tehničnih posegov in konfiguracij. Uporablja se Microsoft Project format.

Dnevnik projektnih zadev	Zapis vseh zadev, ki predvidoma lahko vplivajo na potek ali obseg projekta.
Register tveganj in ukrepov	Zapis vseh predvidenih in opaženih tveganj za uspeh projekta. Določanje stopnje nevarnosti in verjetnosti pojava, definicija vpliva na projekt in ustreznih postopkov.
Register testiranja	Plan in zapisnik testiranja funkcionalnosti.
Zahtevek za uvedbo spremembe	Zahtevek za primer zahteve po spremembi projektnega obsega ali ključnih vsebin projektne dokumentacije.
Obrazci za sprejem faz in končne rešitve	Določila pogojev za zaključek projekta. Njihovo sprejetje pomeni, da so vse funkcionalnosti dobavljene v skladu s SOW in SAO.

4.5.2 Shematski prikaz rešitve

Shema na sliki 26 prikazuje fizični načrt rešitve in medsebojno komunikacijo glavnih komponent po prehodu sistema v produkcijsko okolje. Ponazorjene so vse poti medsebojne interakcije med CA Admin strežniki za delovni tok in oskrbo uporabnikov (interaktivni strežnik) ter kadrovsko aplikacijo in spletnim CA Admin strežnikom, kot komponentami za vnos podatkov in upravljanje z izvajanjem procesov. Prikazane so tudi povezave na imeniški strežnik ter ciljne, upravljane aplikacije.



- **Slika 26. Shematski prikaz logičnih povezav med komponentami predlagane rešitve.**

4.5.3 Sistemske zahteve

V naslednji tabeli so prikazane sistemske in konfiguracijske zahteve, ki morajo biti zadovoljene za postavitev strežnika.

Strežnik	**Zahteve**
"CA Admin Servers"	Naslednji porti so v uporabi in morajo biti odprti na strežniku in internem požarnem zidu: • 20389 LDAP port za CA Admin • 20390 LDAP over TLS port za CA Admin Server • 20391 LDAP port za CA Admin Administrative Directory • 20392 LDAP over TLS za CA Admin Administrative Directory • 20393 LDAP port za CA Admin zalogo operacij • 20394 LDAP preko TLS port za CA Admin zalogo operacij • 20395 SNMP port za CA Admin Administrative Directory • 20396 Console port za CA Admin Administrative Directory • 20397 SNMP port za CA Admin zalogo operacij • 20398 Console port za CA Admin zalogo operacij • 20399 LDAP port za CA Admin usmerjevalnik • 20400 SNMP port za CA Admin usmerjevalnik • 20401 Console port za CA Admin usmerjevalnik • 21391 LDAP port za CA Admin spletni vmesnik delovnega poteka • 21392 LDAP preko TLS port za CA spletni vmesnik delovnega poteka • 443 HTTPS port
"Mainframe"	DSI Konfiguracija: • **IP Address/ Name** določa IP naslov z/OS sistema. • **Admin ID** identificira uporabnikov ID, ki ga dobi pri uporabnikovem logiranju v UNIX System Services (USS). To kreira namestitveni imenik in nalaganje izvršljivih modulov. • **Admin Pswd** geslo za Admin ID. • **HFS Directory** ugotavlja imenik, kjer bo CA DSI inštaliran. • **ProcLib** ugotavlja podatkovni niz, kjer so procedure STC naložene in generirane. Privzet je *SYS1.PROCLIB*. • **Proc Name** *SECV3*. • **Number of Threads** *32*. • **Port** *390*.

4.6 Kakovostni atributi

- Zanesljivost:
  Modul CA Admin uporablja nadgradljiv X.500 imenik kot podatkovni repozitorij za navidezni imenik. Rešitev ima možnost, da upravlja pričakovano število uporabnikov. Drugače imenik uporablja podatkovno bazo z uporabo dvofaznega zapisovanja (angl. *two phase commit*), da zagotovi integriteto transakcij. Modul CA Admin bo

konfiguriran za uravnoteženje bremena (angl. *load balancing*) in visoko dostopnost, da poskrbi za razširjeno zanesljivost in razpoložljivost.

- Razpoložljivost:
  Zaradi nemotenega delovanja med intervali največje obremenjenosti, se izdelava varnostne kopije CA Admin strežnikov izvaja ponoči. Kontrolne točke in datoteke varnostnih kopij so shranjene na lokalnih medijih za ponovno vzpostavitev (angl. *Disaster recovey*). CA Admin Servers tedensko izvršuje popolno varnostno kopijo.

- Uporabnost:
  Sistem za podporo je na voljo vse dni v tednu in se zavezuje, da bo poskrbel za posodobitve in kakršnekoli težave.

4.7 Testiranje uporabniških operacij

Da bi preverili funkcionalnost in rezultate nove rešitve, smo definirali množico testov za vsako metodo/funkcijo novega sistema. V nekaterih primerih smo različne primere uporabe testirali z istimi testi. V nadaljevanju so bolj podrobno opisani in prikazani testi, ki smo jih razdelili v 9 podskupin.

Upravljanje uporabniških računov (testi od 1-6):

T.1 Ustvarjanje računov - preverjamo, ali je uporabniški račun ustvarjen v CA Admin sistemu.

T.2 Spreminjanje vloge računov - preverjamo, ali lahko globalnemu uporabniku spreminjamo vloge v modulu CA Admin.

T.3 Deaktivacija računa – preverjamo, ali so prepovedi globalnih uporabnikov prikazani v končnem sistemu prepovedanih računov pridruženih globalnem uporabniku.

T.4 Ponovna aktivacija računa - preverjamo, ali se reaktivacija izvede tudi v končnem sistemu računov, pridruženih globalnim uporabnikom, ki so bili reaktivirani.

T.5 Brisanje računa – preverjamo, ali se brisanje uporabnikov izvede v končnem sistemu računov, pridruženem globalnem uporabniku.

T.6 Preverjanje vseh uporabniških vmesnikov – ponavljanje testov od 1 do 5 z uporabo CA Admin manager vmesnika.

Glavni koraki testiranja upravljanja uporabniških računov:

1. Uporabi IA Manager za ustvarjanje novega globalnega uporabnika.
2. Dodeli zunanjega uporabnika globalnemu.
3. Preveri, ali so ustvarjeni računi z dodeljevalno vlogo.
4. Preveri, ali so obvestila poslana skrbniku aplikacij ter preveri, ali so vsa ta stanja zabeležena v vmesniku CA Admin delovnega toka.
5. Preveri ažuriranje in brisanje.
6. Dodeli uporabniku vlogo zaposlenega in preveri, ali so se spremenile pravice.

7. Naredi iste korake in uporabi Admin Manager.

Zahteva uporabnika za dostop (test 7):

T.7 Upravljanje z imenskim prostorom – preverjamo, ali se ročno oskrbovanje lahko pošlje CA Admin sistemu.

Glavni koraki testiranja uporabnikovih zahtev za dostop:

1. Uporabi IA Manager in zahtevaj dodajanje testnega uporabnika.
2. Preveri potrdilo SMNT notifikacije zahteve modula CA Admin (skrbnik aplikacij).
3. Preveri, ali se je obvestilo registriralo v modulu CA Admin in ali je status sledenja ažuriran pravilno.

Ponastavitev gesla (test 8):

T.8 Samopostrežna ponastavitev gesla – preverjamo, ali samopostrežni sistem omogoča končnemu uporabniku ponastavitev gesla na končnem sistemskem računu.

Glavni koraki testiranja ponastavitve gesla:

1. Zaženi spletni vmesnik CA-IM Self Service.
2. Začni proces "pozabljeno geslo".
3. Odgovori pravilno na vprašanje za samo-avtentifikacijo.
4. Preveri, ali uspešno končana samo-avtentifikacija dovoli ponastavitev gesla.
5. Spremeni geslo in ga uporabi v sistemu, da preveriš njegovo pravilno delovanje.

Samopostrežna administracija (test 9):

T.9 Samopostrežna administracija – preverjamo, ali samopostrežni sistem omogoča končnemu uporabniku upravljanje svojega računa.

Glavni koraki testiranja samopostrežne administracije:

1. Zaženi spletni vmesnik IAM Self Service.
2. Izberi možnost "začetek delovnega toka".
3. Vnesi zahtevane informacije.
4. Preveri, ali se je pregledala in odobrila zahteva za delovnim tokom.

Delegirana administracija (test 10):

T.10 Delegirana administracija - preverjamo, ali se globalni uporabniki lahko ustvarijo, spreminjajo, prekinejo, ponovno aktivirajo in brišejo preko brskalnika.

Glavni koraki testiranja delegirane administracije:

1. Zaženi vmesnik CA Identity Manager in odpri določenega uporabnika.
2. Ustvari globalnega uporabnika.
3. Spremeni račun globalnega uporabnika.
4. Prepoved dostopa do računov globalnega uporabnika.
5. Ponovna aktivacija dostopa do računov globalnega uporabnika.
6. Brisanje računov globalnega uporabnika.
7. Za vsak korak preveri, ali so se akcije izvedle v modulu CA Admin.

Poročila o statusih uporabniškega računa (test 11):

T.11 Rešitev revizije upravljanja identitet – preverjamo, ali se ustvarjajo poročila uporabniškega računa za uporabnike procesirane z modulom CA Admin.

Glavni koraki testiranja poročila uporabniškega sistema:

1. Zaženi CA Admin Report Explorer.
2. Izberi merila poročil.
3. Generiraj podatkovno bazo poročil.
4. Zaženi uporabniško poročilo.
5. Preveri, ali so pričakovani podatki v poročilu.

Upravljanje avtoritativnega uporabniškega vira (test 12):

T.12 Upravljanje avtoritativnega uporabniškega vira – simuliramo delovanje kadrovskega sistema z dodajanjem uporabnika v kadrovski sistem.

Glavni koraki testiranja upravljanja avtoritativnega uporabniškega vira:

1. Simuliraj delovanje kadrovske ali ročno dodajanje uporabnika v kadrovsko.
2. Preveri, ali je zahteva za delovni tok inicializirana v modulu CA Admin.
3. Preveri, ali so pravilni podatki sprejeti.
4. Zbriši uporabnika iz kadrovske.
5. Preveri zahtevo delovnega toka in ali je brisanje izvršeno.

Upravljanje aplikacij in strežnikov (testi 13-19):

T.13 Delovni tok običajnih administrativnih nalog - preverjamo pravilno delovanje delovnega toka pregleda skladnosti varnosti aplikacije, novih imenskih prostorov in zbrisanih imenskih prostorov.

T.14 Pridobivanje podatkov - preverjamo, ali so aplikacije, ki jih upravljamo, prikazane v modulu CA Admin.

T.15 Brskanje podatkov - preverjamo, ali so aplikacijski računi, ki jih upravljamo, prikazani v modulu CA Admin.

T.16 Povezovanje uporabniških računov z globalnim uporabnikom - preverjamo, ali se lahko aplikacijski računi pridružijo obstoječim globalnim uporabnikom v modulu CA Admin.

T.17 Upravljanje s politikami – preverjamo, ali CA Admin politike lahko uporabimo kot predloge za pravilno ustvarjanje uporabniških računov v upravljanih sistemih.

T.18 Upravljanje z vlogami - preverjamo, ali CA Admin politike lahko uporabimo kot predloge za pravilno ustvarjanje uporabniških vlog (ali skupin) v upravljanih sistemih.

T.19 Upravljanje s pristopnimi pravicami – preverjamo, ali omejene pravice dostopa do modula CA Admin lahko pridružimo globalnem uporabniku preko modulovega varnostnega profila.

Glavni koraki testiranja upravljanja aplikacij in strežnikov:

1. Začni delovni tok za novo aplikacijo in zahtevo preizkusa skladnosti pridruženega upravljanja identitet.
2. Preveri, ali je obvestilo generirano in pravilno sprejeto.
3. Začni delovni tok za obvestilo novega imenskega prostora in preveri, ali je to sprejeto.

Definiranje/vzdrževanje politike upravljanja identitet, procesov in lastnikov (test 20):

T.20 Vzdrževanje politike upravljanja identitet – preverjamo definiranje politike upravljanja identitet, procesov in lastnikov.

Glavni koraki testiranja politike vzdrževanja upravljanja identitet:

1. Zaženi proces delovnega toka za verifikacijo politik in preveri, ali je sproženo obvestilo.
2. Dodeli testnega uporabnika kot odobritelja za pridobivanje pristopa za določeno aplikacijo in preveri, ali politika dovoli to vlogo.
3. Definiraj administrativni profil in preveri, da ima globalni uporabnik dodeljen v ta profil omejene pravice.

5 Zaključek

V diplomski nalogi sem opisal rešitev projekta vpeljave sistema za upravljanje z identitetami. Izvedena je bila z aplikacijo CA Identity Manager. Predstavil sem poslovne zahteve in operativne cilje organizacije, ki se je odločila za rešitev za upravljanje identitet. Naloga zajema celoten proces vpeljave rešitve od posnetka trenutnega stanja, do dejanske implementacije novih procesov in tehnologij.

V organizaciji do uvedbe rešitve ni obstajal koncept globalne identitete, ki bi bil povezljiv z vsemi računi in pravicami, ki jih uporabnik ima na ključnih informacijskih sistemih. Ravno tako sta vsem procesom dodeljevanja, spreminjanja in odvzema pravic manjkali dve kritični komponenti – sledljivost in dokazljivost.

Večji izzivi s katerimi smo se srečali pri izvedbi projekta so bili neobveščenost IT osebja o konceptih in možnostih tehnologije, upiranje lokalnih administratorjev centralizaciji upravljanja, ter težavnost standardizacije politik in procesov s številnimi praktičnim izjemami. Po izvedenih fazah definiranja in zapisovanja globalne politike, planiranju fizične in logične arhitekture rešitve ter implementacije in integracije sistema, so bili doseženi vsi projektni cilji, s čimer je bilo zadoščeno poslovnim zahtevam naročnika.

Rešitev je bila ocenjena kot uspešna in bo kot takšna omogočala nemoteno podporo vseh procesov upravljanja z identitetami ter tudi zadostno razširljivost za vpeljavo morebitnih organizacijskih sprememb.

Seznam uporabljenih virov

[1] CA Identity Manager Operations Guide r8.1, K02764-1E, March 3, 2006
https://support.ca.com/cadocs/g0/g011121e.pdf

[2] CA Identity Manager configuration Guide r8.1, March 3, 2006
https://support.ca.com/cadocs/g0/g011131e.pdf

[3] CA eTrust Admin Administrator Guide r8.1 SP2, 2006
https://support.ca.com/cadocs/g0/g007164e.pdf

[4] CA eTrust Admin Implementation Guide r8.1 SP2, second edition, 2006
https://support.ca.com/cadocs/g0/g006986e.pdf

[5] CA eTrust Directory Administrator Guide r8.1 second edition, 2005
https://support.ca.com/cadocs/g0/g010302e.pdf

[6] CA eTrust Directory Release Summary r8.1 second edition, 2005
https://support.ca.com/cadocs/g0/g010322e.pdf

Izjava o samostojnosti dela

Izjavljam, da sem diplomsko nalogo izdelal samostojno pod mentorstvom izr. prof. dr. Mihe Mraza in somentorstvom doc. dr. Mire Trebar. Izkazano pomoč drugih sodelavcev sem v celoti navedel v zahvali.

Datum Kandidat