UDC: 004.7 INFO M: str. 12-16

UPRAVLJANJE MREŽNIM SERVISIMA U VISOKOŠKOLSKOJ USTANOVI
MANAGEMENT OF NETWORK SERVICES INSTITUTION OF HIGHER EDUCATION

Vladimir Vujin

REZIME: U radu je prikazan model sistema za upravljanje mrežnim servisima u visokoškolskoj ustanovi. Model mrežnih servisa treba da omogućiti integraciju heterogenih mrežnih sistema i servisa, jednostavno i efikasno upravljanje, upotrebu i praćenje mrežnih servisa u visokoškolskoj ustanovi (fakulteti, visoke škole strukovnih studija), prilagođenih za primenu u uslovima visokoškolskog obrazovanja u Republici Srbiji.
KLJUČNE REČI: mrežni servisi, digitalni identitet
ABSTRACT: The paper presents a model system for the management of network services in the higher education institution. The main goal model of network services is to enable integration of heterogeneous network systems and services, simply and efficiently manage, use and monitoring of network services in higher education institutions (faculties, high school vocational studies), adapted for use in conditions of higher education in the Republic of Serbia.
KEY WORDS: network services, digital identity

1. UVOD

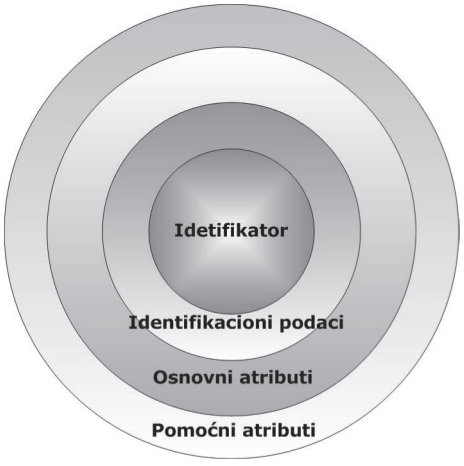
Razvoj informacionih i komunikacionih tehnologija kao i računarske i telekomunikacione opreme omogućio je pojavu velikog broja novih mrežnih servisa. Uključivanje novih servisa u mrežni informacioni sistem doprinosi podizanju kvaliteta naučno-nastavog i istraživačkog procesa, a sa druge strane negativno se odražava na sigurnost, pouzdanost, dostupnost i upravljivost mrežne infrastrukture visokoškolske ustanove.

Mrežni informacioni sistem koji obezbeđuje sve veći broj servisa, zahteva jasno definisan, pouzdan i efikasan sistem za upravljanje digitalnim identitetima. Sistem za upravljanje digitalnim identitetima je neophodan i zbog činjenice da su korisnici iz akademske i istraživačke zajednice sve mobilniji i traže pristup Internetu i mrežnim servisima na koje su navikli i izvan granica svojih ustanova, akademske mreže, zemlje. Bolonjski proces u Evropi upravo doprinosi takvom trendu - posebno među studentskom populacijom.

2. UPRAVLJANJE DIGITALNIM IDENTITETIMA

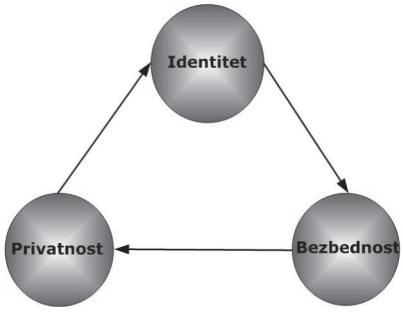
Identitet je jedinstveni niz karaktera koji jednoznačno označava osobu ili servis. Digitalni identitet je skup podataka koji prezentuju atribute, sklonosti i osobine subjekta. Digitalnim identitetom se smatra skup informacija koji je poznat o određenom entitetu. Subjekt ili entitet predstavlja osobu, grupu ljudi, organizaciju, programski alat ili bilo koji drugi entitet koji zahteva pristup mrežnim resursima.

- **Identifikator** – Deo informacije koja jedinstveno identifikuje predmet identiteta unutar datog konteksta.
- **Identifikacioni podaci** – Privatni ili javni podaci koji bi mogli biti korišćeni da se dokaže autentičnost identiteta. Identifikacioni podaci predstavljaju dokaz da određeni subjekt odgovara identitetu za koji se izdaje.
- **Osnovni atributi** – Podaci koji pomoćno opisuju identitet. Osnovni atributi mogu se koristiti pomoću brojnih poslovnih aplikacija.
- **Pomoćni atributi** – Podaci koji pomoćno opisuju identitet, navode se i koriste unutar specifičnog konteksta u kojem se identitet koristi.



Slika 1. – *Digitalni identitet*

Razvoj elektronskog poslovanja koje se temelji na pružanju usluga, u prvi plan stavlja digitalni identitet korisnika usluge i celokupni proces upravljanja digitalnim identitetima. Pojmovi anonimnosti i privatnosti, u suprotnosti su sa transakcijama kojima se zahteva prodaja, kupovina ili pristup određenim servisima gde je otkrivanje informacija o identitetu neophodno.

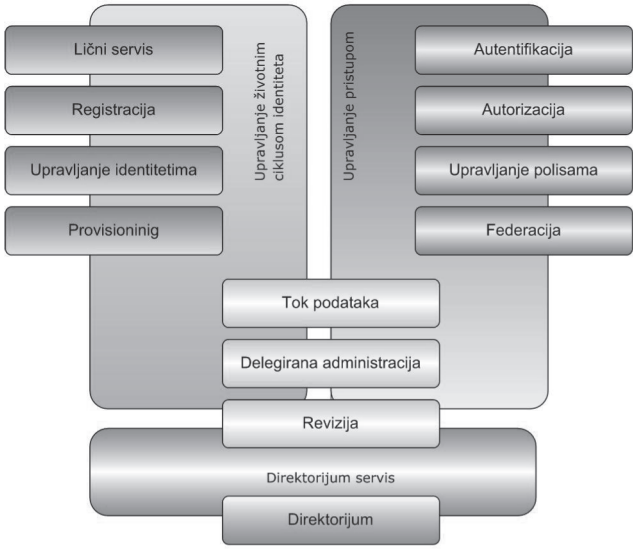


Slika 2. – *Veza između identiteta, bezbednosti i privatnosti*

Upravljanje digitalnim identitetom je skup procesa koji omogućuju visokoškolskoj ustanovi efikasnije upravljanje mrežnim servisima i osiguravaju celovitu sigurnosnu infrastrukturu. Konsolidovanjem podataka o entitetima iz različitih izvora, sistem za upravljanje identitetima može unaprediti sigurnost dodeljivanjem pristupa kroz modularno aplikativno okruženje i smanjiti troškove administracije i održavanja informacionog sistema. Sa implementiranom infrastrukturom sistema za upravljanje identitetima, visokoškolske ustanove mogu se razviti novi poslovni model za komunikaciju i pristup servisima.

Sistem za upravljanje identitetima obuhvata tri ključne tehnološke komponente:

- Upravljanje životnim ciklusom identiteta
- Upravljanje pristupom
- Direktorijum servis

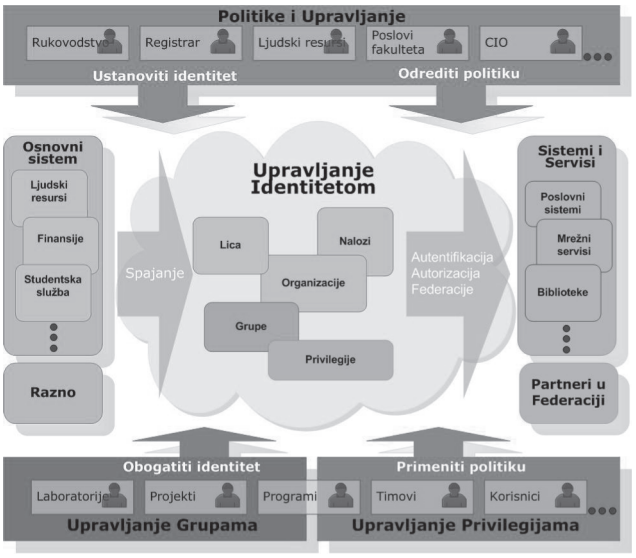


Slika 3. – *Sistem za upravljanje identitetima*

3. MODEL SISTEMA ZA UPRAVLJANJE IDENTITETIMA

Sistem za upravljanje identitetima treba da obezbedi da se pravim korisnicima da pravo pristupa podacima i servisima. U prošlosti, ovaj je sistem implementiran kao sistem sa duplim identitetima koji su distribuirani širom sistema. Dodavanjem novih servisa u ovakvu informacionu infrastrukturu ispoljilo je probleme vezane za bezbedno upravljanje duplim identitetima.

Rešenje ovoga problema je da se koristi isti digitalni identitet za sve aplikacije i servise. Model sistema za upravljanje identitetima (Slika 4.) prikazuje da integracija izvornih podataka sa sistemima i servisima u sistem za upravljanje identitetima omogućuje da se sve politike i procedure mogu primeniti na jednom centralnom mestu. Primena ovakvog modela pojednostavljuje upravljanje i pristup i povećava bezbednost procesa upravljanja identitetima.



Slika 4. – *Model sistema za upravljanje identitetima*

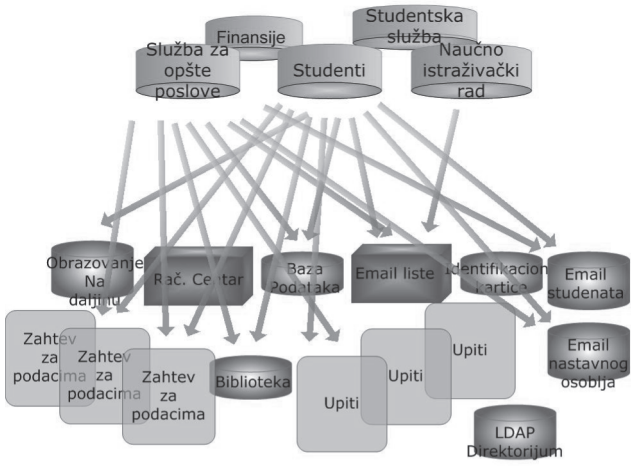
Prvi korak u izgradnji infrastrukture sistema za upravljanje identitetima je prikupljanje podataka o entitetima distribuiranih širom sistema, zatim donošenje odluke koji podaci su relevantni i na kraju uređivanje i smeštanje informacija o svakom entitetu u jedan zapis koji predstavlja digitalni identitet.

Sa konsolidacijom informacija o identitetima, upravljanje sistemom postaje efikasnije, zato što infrastruktura sistema za upravljanje identitetima postaje veza između institucionalnih procesa i vlasnika resursa i tehnoloških operacija. On takođe omogućava skaliranje operacija informacionih tehnologija čime se ostvaruje zahtev da razvojem procesa i servisa, prateće promene nastaju na samo jednom mestu, u sistemu za upravljanje identitetima.

Uobičajeni zahtevi za centralizovano upravljanje identitetima i centraliziovano upravljanje korisničkim pravima:

- Upravljanje centralnom bazom sertifikovanih dozvola koje su autentične
- Potvrda usklađenosti sa regulativom
- Definsani postupci za pristupne zahteve i odobrenja
- Podrška za upravljanje radnim funkcijama
- Automatizovano kreiranje korisničkih naloga i dodela prava
- Automatizovano gašenje korisničkih prava
- Uspostavljanje upravljačkog sistema radi jednostavnije administracije
- Uspostavljanje jedinstvenog sistema identifikacije za sve aplikacije i servise

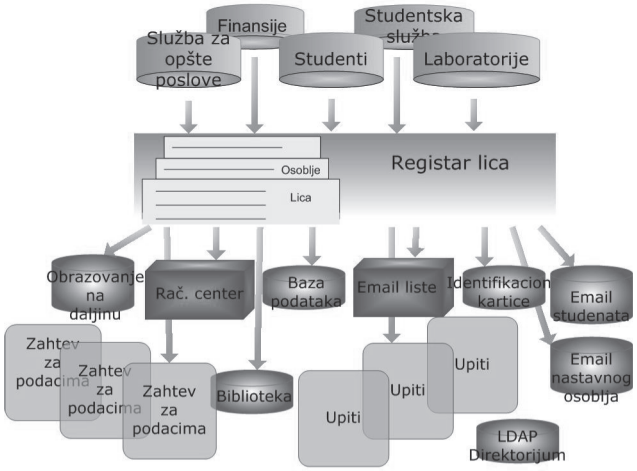
Upravljanje iz jedne tačke omogućava konsolidovano logovanje i konzistentan pogled na pristupna prava i potrebe pojedinaca i sistema. Ovakav pristup omogućava transparentan način primene, praćenja i sprovođenja politike i odluka u tehnološku infrastrukturu. Ono takođe pruža mogućnost praćenja istorije kome je i čemu je odobren pristup kao i jedno mesto za reviziju, izveštavanje i za praćenje bezbedonosnih događaja.



Slika 5. – *Model organizacije bez sistema za upravljanje identitetima*

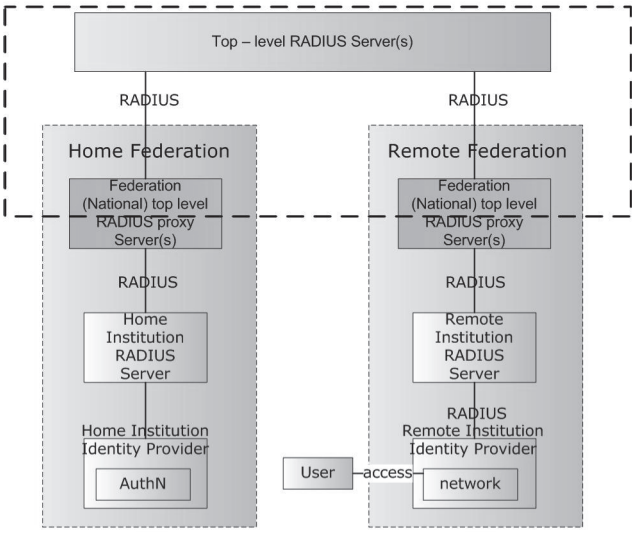
Sa implementiranim sistemom za upravljanje identitetima u visokoškolskoj ustanovi moguće je iskoristiti ključne prednosti kao što su: unapređena sigurnost, smanjenje troškova administracije i unapređenje produktivnosti korisnika.

- Unapređena sigurnost – uklanjanjem kašnjenja u implementaciji prava pristupa radi promena identiteta i pravila
- Manji troškovi – automatizacijom upravljanja životnim ciklusom identiteta
- Unapređena produktivnost – implementacija Singl sign–on koncepta povećava produktivnost korisnika.



Slika 6. – *Model organizacija sa sistemom za upravljanje identitetima*

Koristi od uvođenja sistema za upravljanje identitetima proizilaze iz centralizovane administracije korisnika koja omogućuje administratorima dodeljivanje, zabranu i rukovanje pristupom prema resursima za sve korisnike sa centralne lokacije čime se trenutno distribuiraju homogena pravila kroz sve službe i lokacije u visokoškolskoj ustanovi. Istovremeno primenjujući pravila prema svim korisnicima, visokoškolska ustanova može smanjiti mogućnost ljudske greške i time se zaštititi od skupih posledica koje se mogu dogoditi usled davanja prava pristupa prema kritičnoj aplikaciji neovlašćenim korisnicima ili neispravnom zabranom pristupa nekom resursu. Centralizovani sistem za upravljanje identitetima omogućava visokoškolskim ustanovama stvaranje i sprovođenje pravila, dodeljivanje prava krajnjim korisnicima kao što je pravo da sami menjaju svoje lozinke i da sami sebi dodele prava nad resursima koji nisu od velikog sigurnosnog značaja. Centralizovani sistem za upravljanje identitetima omogućuje korisnicima postavljanje zahteva prema različitim resursima, gde sistem može automatski dodeliti pravo na osnovu pravila i uloge korisnika ili upotrebiti workflow mehanizam za traženje odobrenja odgovorne strane.



Slika 7. – *Enterprise direktorijum*

Na slici 7. prikazan Enterprise diretorijum i način na koji se informacije o identitetu izdvajaju iz postojećeg sistema, kako se transformišu putem metadireketorijum procesa i smeštaju u direktorijum i na taj način ih čine dostupnim za korišćenje od strane sistema.

Postoje tri uobičajene komponente Enterprise direktorijum arhitekture:

1. registar – predstavlja bazu podataka o svakom entitetu od značaja,
2. interfejs za korisničke aplikacije – obično LDAP direktorijum ili autentifikacioni server, kao što je Kerberos i
3. metadirektorijum infrastruktura – koja kontroliše tok informacija između sistema slogova, enterprise direktorijum komponente i korisničke aplikacije.

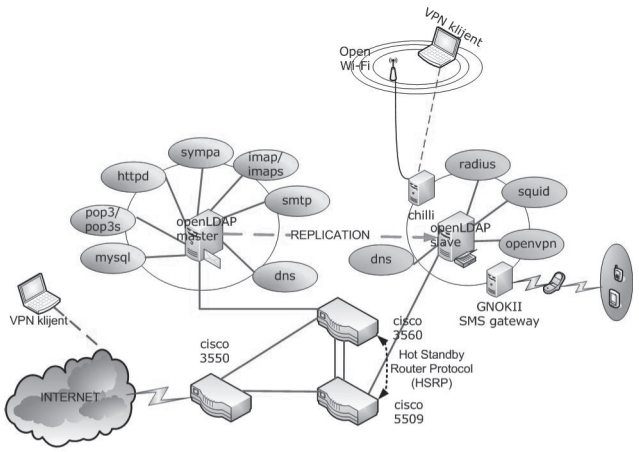
Enterprise direktorijum predstavlja skup alata koji upravljaju protokom informacija. Metadirektorijum procesi u ovakvom sistemu pružaju informacije o servisima na osnovu jedinstvenih pravila koja definišu elemente provere identiteta i autorizacije i predstavljaju primarno mesto gde se proverava identitet između različitih sistema. Enterprise direktorijum generalno nije samostalan servis. On predstavlja sredstvo za objavljivanje podataka na jednostavan i lako dostupan način. Kao takav, jedan ili više baza podataka dostavljaju podatke za skladištenje u direktorijum. Postoje takođe i podaci koji postoje samo u direktorijumu. Kao što je prikazano na slici

(Slika 7.), Enterprise direktorijum obuhvata veliki broj usluga i procesa i obično predstavlja više od jednog fizičkog sistema. Podaci, ulazi u sistem, prolaze kroz pridruženi proces da bi se sjedinili sa ispravnim identifikatorom, zatim se upisuju u registar lica. Registar lica može poslužiti kao referenca identifikatora za druge sisteme.

4. FEDERALNI MODEL SISTEMA ZA UPRAVLJANJE IDENTITETIMA

Sprovođenjem Bolonjskog procesa sve veći broj studenta, predavača i saradnika je u statusu mobilnih programa u okviru Evropske visokoškolske institucije. Stvaranje federacije između sistema za upravljanje identitetima visokoškolskih ustanova je osnova koja obezbeđuje mobilnost korisnika i dozvola za razmenu sadržaja i usluga između institucija.

Pri dizajniranju sistema za upravljanje identitetima posebna pažnja usmerena je na potrebu integracije sa sistemom za upravljanje identitetima u Evropskim visokoškolskim institucijama koja promovišu pokretljivost i deljenje sadržaja i usluga Akademske zajednice. Sistem za upravljanje identitetima dostavlja informacije o korisniku Single sign-on aplikacijama različitih visokoškolskih ustanova, čime se ostvaruje da jedan identitet omogućava zajednički pristup. Kada korisnik želi da pristupi kontrolisanom resursu, skup atributa koji je dinamički prikupljen, predaje se aplikaciji. Na osnovu tog skupa atributa, aplikacija može da donese odluku da odobri ili odbije pristup korisniku, ili može da se prilagodi za korisnika.

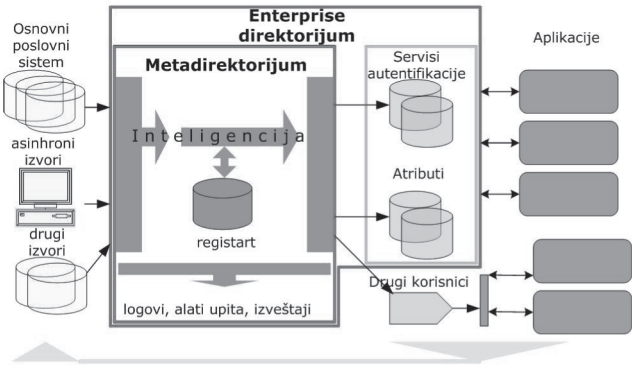


Slika 8. – *Federalni model sistema*

Na ovaj način federacija omogućuje sigurno deljenje informacija sa spoljnim sistemima organizacijama koje upravljaju sa identitetima spoljnih korisnika. Bez ove funkcionalnosti administratori moraju održavati odvojeni direktorijum za sve spoljne korisnike i ručno upravljati podacima o korisnicima. Sistem ujedinjenih identiteta omogućava korisnicima na jednom domenu da pristupe resursima na drugom domenu bez dodatnog predstavljanja. Uobičajeni, poseban poslovni odnos, opravdava poverenje koje će biti osnova za pružanje pristupa kroz mrežne granice između različitih visokoškolskih ustanova.

5. MODEL UPRAVLJANJA MREŽNIM SERVISIMA NA FON-U

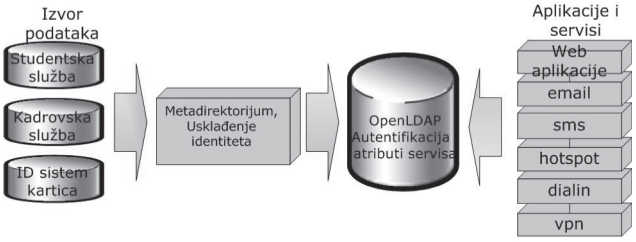
Mrežni informacioni sistem FON-a dizajniran je tako da pruža najbolje moguće okruženje za naučno-istraživački rad i obrazovanje studenta kroz integrisane mrežne servise koji omogućuju svim studentima, nastavnom osoblju i radnicima FON-a da komuniciraju jedni sa drugima i da imaju mogućnost pristupa informacijama sa bilo kog mesta u bilo koje vreme.



Slika 9. – *Mrežni servisi FON-a*

Skup Internet servisa u FON-ovoj računarskoj mreži je koncipiran tako da bude što modularniji. Da bi se takva celina uspostavila, bilo je potrebno oformiti je oko jednog, centralnog servisa, koji bi pružao svim ostalim servisima sistema ključne informacije, a to su podaci o entitetima. Pri tome, ova centralna komponenta mora biti takva da se može lako administrirati, može sadržati neograničen broj proizvoljnih podataka o entitetima, uz mogućnost lakog proširenja skupa entiteta i brzo nalaženje potrebnih informacija.

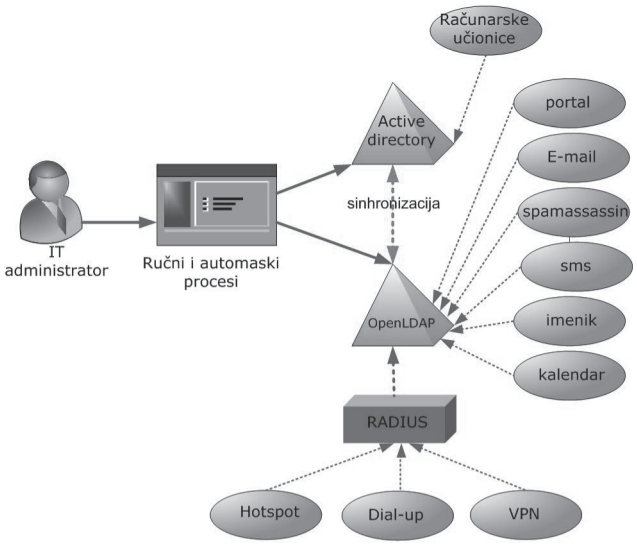
Sistem za upravljanje identitetima na FON-u trenutno postoji kao OpenLDAP direktorijum servis koji omogućuje verifikaciju autentičnosti putem šifrovanih lozinki za nekoliko većih aplikacija. Da bi ovakav sistem mogao da funkcioniše važno je definisati odgovarajuću šemu, odnosno precizan popis objekata i atributa sa jasnim opisom, semantikom i sintaksom. Administrator i svaki servis koji pristupa i menja LDAP direktorijum mora se pridržavati postojećim definicijama objekata i atributa.



Slika 10. – *Model sistema za upravljanje digitalnim identitetima na FON-u*

Model mrežnih servisa na FON-u koristi postojeće UNIX i Windows infrastrukture, ali se ostvaruje interoperativnost između UNIX Kerberosa i Kerberosa Aktivnog Direktori-

juma, stvarajući međusobno poverenje. Windows klijenti i UNIX klijenti se autentifikuju na sopstveni KDC i ukoliko je poverenje obostrano, dobijaju poverenje od radnih stanica i servera i sa druge strane.



Slika 11. – *Upravljanje mrežnim servisima FON-a*

UNIX korisnici, kada su autentifikovani na UNIX KDC, mogu pristupiti servisima (aplikacijama) Windows okruženja bez da moraju da se ponovo autentifikuju. Windows KDC veruje UNIX KDC autentifikovanim akreditacijama i tako dozvoljava pristup Windows servisima bez zahtevanja autentifikacije korisnika.

Model mrežnih servisa na FON-u zahtevao je minimalnu modifikaciju infrastrukture a ipak je omogućio i Windows i UNIX korisnicima da pristupe Kerberizovanim aplikacijama u bilo kom okruženju bez potrebe da učestano unose korisničko ime i lozinku. UNIX korisnici koriste postojeći metod autorizacije.

6. ZAKLJUČAK

U radu je prikazano kako se primenom savremenih informaciono-komunikacionih tehnologija doprinosi efikasnijem i fleksibilijem sistemu rada visokoškolske ustanove.

Zbog svoje modularnosti, celokupan sistem ali i svaki od servisa se jednostavno može prilagoditi bilo kojoj visokoškolskoj ustanovi, uz jednostavnost centralizovanog upravljanja i revizije. Zbog ovoga, skup mrežnih servisa, kako je implementiran na FON-u, predstavlja jednu od najboljih celina koja se mogu napraviti uz upotrebu različitih otvorenih softverskih rešenja, a da pri tome ona ne gubi nimalo od svoje upotrebljivosti, pouzdanosti, fleksibilnosti i lakoće korišćenja i održavanja.

LITERATURA

[1] Jeremy Moskowitz and Thomas Boutell, Windows and Linux Integration: Hands-on Solutions for a Mixed Environment, Sybex, 2005.
[2] Gerald Carter, LDAP System Administration, O'Reilly, 2003.
[3] Clayton Donley, LDAP Programming, Management and Integration, Manning Publications Co., 2003.
[4] Matt Butcher, Mastering OpenLDAP, Packt Publishing Ltd., 2007.
[5] Phillip J Windley, Digital Identity, O'Reilly, 2005.
[6] David Birch, Digital Identity Management, Gower Publishing Limited, 2007.
[7] Jason Garman, Kerberos: Definitive Guide, O'Reilly, 2003.

Mr Vladimir Vujin, Fakultet organizacionih nauka Univerziteta u Beogradu,
vladimir.vujin@fon.rs
Oblasti interesovanja: Internet tehnologije, Identity management, Cloud Computing