Marko Vulić[1], Marko Ranković[2], Vojkan Vasković[3]
[1]Stipendista Ministarstva za nauku i tehnološki tazvoj, Fakultet organizacionih nauka u Beogradu
[2]EuroPlanet d.o.o, Beograd
[3]Beogradska Poslovna Škola

Upravljanje identitetom u savremenom poslovanju - primer primene Cloud sistema

UDK: 004.42:004.738.52 ; 004.738.5:005.41
DOI: 10.7595/management.fon.2012.0008 (english version)

Upravljanje identitetom jedan je od najvećih izazova na Internetu danas, uglavnom zbog sve većeg broja usluga i mogućih zloupotreba. Digitalizacija informacija znatno je olakšala prikupljanje, skladištenje i deljenje velikih količina podataka, ali je takođe doprinela i razvoju rizika vezanih za privatnost u sistemima upravljanja. U radu je prikazan koncept upravljanja identitetom, u kojem su definisani elementi životnog ciklusa digitalnog identiteta. Rad opisuje model upravljanja identitetom, prikazujući najvažnije elemente modela, odnos menadžmenta identiteta, kao i arhitekture sistema. Prikazani su neki od najznačajnih standarda za upravljanje identitetom i paterni u Cloud sistemu.

Ključne reči: upravljanje identitetom, model upravljanja identitetom, standardi, bezbednost podataka, Cloud paterni.

1. Uvod

Identitet se definiše kao skup ličnih karakteristika koje pojedinca čine pripadnikom grupe. Spoznaja identiteta iz ljudske perspektive se posmatra kroz osećaj pripadnosti i osećaj odbačenosti. [1]

Upravljanje identitetom obuhvata tehnologiju, procese, funkcije i mogućnosti u upravljanju informacijama o identitetu, očuvanja identiteta entiteta i poboljšanja složenosti i sigurnosti poslovnih aplikacija. Upravljanje identitetom predstavlja oblast koja se bavi identifikovanjem pojedinaca u sistemu i kontrolom njihovog pristupa resursima u okviru tog sistema, udruživanjem prava korisnika i ograničenjima sa utvrđenim identitetom. [2]

Dve glavne komponente upravljanja identitetom su upravljanje “po” identitetu i upravljanje “od strane” identiteta. Upravljanje po identitetu je proces izdavanja i korišćenja digitalnih identiteta i akreditiva (npr. korisničko ime i lozinka) za autentifikaciju. Upravljanje od strane identiteta kombinuje potvrđen identitet korisnika sa njihovom autorizacijom, kako bi pristup resursima bio odobren. [3]

2. Razvoj i upravljanje identitetom

Identitet kao i digitalni identitet može biti sastavljen iz skupa atributa. Skup atributa čine podskupovi parcijalnih identiteta u različitim životnim dobima.

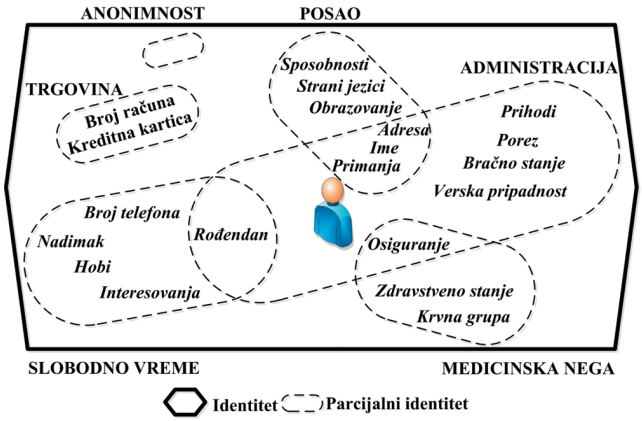
Faze životnog ciklusa parcijalnog identita su [4]:
- *Formiranje parcijalnog identiteta* - kreiranje ili pripisivanje identiteta nekoj ličnosti (pojedincu).
- *Razvijanje parcijalnog identiteta* - korišćenje parcijalnih identiteta kako od strane vlasnika identiteta, tako i od strane drugih.
- *Okončanje parcijalnog identiteta* - brisanje ili suspendovanje parcijalnog identiteta.

Sve prethodno navedene faze se relevantne za formiranje parcijalnih identiteta.

U većini evropskih zemalja detetu se ubrzo po rođenju formiraju jedinstveni identifikatori. Jedan od njih je krštenica koja sadrži ime, prezime, pol, mesto i godinu rođenja, i podatke o biološkim roditeljima. Ovakav vid registracije ne može sprečiti niko, čak ni roditelji jer na taj način dete postaje zvanični građanin Države.

Sledeći zvaničan dokument je zdravstveni karton. U njemu se osim osnovnih podataka o detetu (ime, prezime, pol, datum i godina rođenja) beleži jedinstveni matični broj pod kojim se dete vodi u evidenciji građana i medicinski podaci (visina, težina, podaci o porođaju majke, itd.). Kako dete odrasta tako se tokom godina i sam medicinski karton popunjava sa više podataka. Kada se dete upiše u obdanište, otvara se karton sa ličnim podacima deteta i podacima o njegovim roditeljima. Tokom boravka u obdaništu formira se parcijalni identitet deteta, sa kojim se ono vremenom poistovećuje i počinje da ga živi.

U nameri da posluju sa nekim firmama i kompanijama, roditelji mogu ustupiti prava slikanja svoje dece ili njihovog učestvovanja u snimanjima reklama. Premda se ovakvi materijali retko brišu, digitalni identitet se samo povećava a retko kada, ili čak nikada, ne smanjuje. Za neke od parcijalnih identita može se reći da ne prestaju čak i nakon smrti pojedinca, jer se mogu preneti na drugu osobu (npr. broj socijalnog osiguranja). [4] [5]

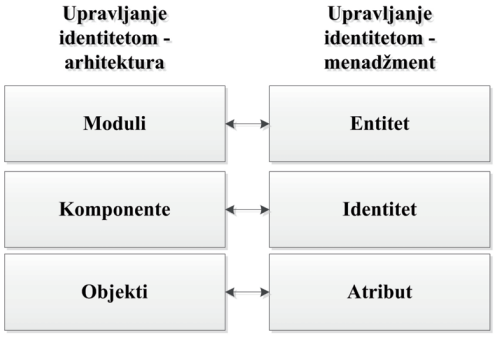


Slika 1 : Parcijalni identiteti [4]

3. Formalni model upravljanja identitetom

Formalni model upravljanja identitetom sastoji se iz ključnih koncepata [6]:

- **Atribut -** Atribut predstavlja karakteristiku u vezi sa entitetom (ime, datum rođenja, generički kod, otisak prsta, itd.)
- **Identitet -** apstraktno predstavljanje entiteta.
- **Delimični identitet -** podskup atributa povezan sa entitetima (ime, starost, broj kreditne kartice) koje pojedinac koristi u interakciji sa drugim učesnicima.
- **Identifikator -** identifikuje različite osobe, mesta ili stvari. Postoje dve vrste identifikatora:
  - *Lični identifikator* - trajni identifikatori povezani sa individualnim ljudskim atributima i atributima koji se teško menjaju ili ne mogu uopšte promeniti (npr. datum rođenja, genetski kod);
  - *Pseudonim* - identifikator povezan sa atributima ili setom transakcija, ali bez stalnog ili ličnog identifikatora.
- **Kontekst -** okolnost u kojoj se nalazi entitet**.**



Slika 2 : Povezanost arhitekture i menadžmenta upravljanja identitetom [7]

4. Osetljivost identiteta

Percepcija podataka, odnosno prihvatanje nekog podatka kao senzitivnog ili ne-senzitivnog je subjektivno. Senzitivnost podataka ne posmatra se samo iz ugla privatnosti, već i kroz njihovu sigurnost. Evropska Unija definisala je posebne kategorije podataka za koje državama članicima nije dozvoljena obrada, osim u posebnim okolnostima: lični podaci koji otkrivaju rasno ili etničko poreklo, političko opredeljenje, versku pripadnost, podaci o zdravlju ili seksualnom životu.

4.1. Osetljivost bazirana na privatnosti

Atributi koji su statični tokom vremena mogu buti senzitivni ako se otkriju iznova i iznova u različitim situacijama, jer na taj način omogućavaju povezivanje srodnih podataka. Otkrivanje statičkih atributa omogućava posmatraču da poveže te situacije i prikupi podatke koji mogu da se koriste za identifikaciju pojedinaca čiji se atributi kontrolišu.

Postoje atributi koje pojedinac ne može sam determinisati (npr. vlastito ime), i oni se mogu svrstati u inicijalne atribute. Takođe se neke vrednosti atributa nasleđuju, kao što je DNK od roditelja ili porodično prezime. Parcijalni identiteti deteta su unapred određeni od strane roditelja, jer ono još uvek nije u stanju da samo donosi odluke.

Samoinicijativna promena vrednosti atributa pojedincu može omogućiti da sam kontroliše svoj identitet, ali to ipak nije uvek moguće kao što se vidi na primeru statičnih atributa. Sledi da autonomija pojedinca može biti ograničena vrednošću samih atributa. Neke atribute je nemoguće otkriti ako se istovremeno ne otkriju i neki dodatni podaci koji su vezani za sam atribut. Ponekad je teško odvojiti te dodatne informacije na stranu, i dešava se da pojedinci nisu sposobni da otkriju te dodatne informacije ako se od njih zatraži da pronađu neke podatke.

Na pojedinca mogu uticati vrednosti atributa ili sam atribut ako je u mogućnosti da mu obezbedi jedinstvo unutar grupe. Pojedinac može ostati anoniman kao i do tada, ili se prepoznati u nekom kontekstu čime njegova privatnost biva ugrožena. Na primer, uspostavljanje direktnog kontakta putem telefona ili e-mail-a može se tumačiti kao ugrožavanje privatnosti. Čak i da se ne uspostavi direktan kontakt sa pojedincem, na njega je moguće ostvariti negativan uticaj putem diskriminacije.

Kada je reč o diskriminaciji obično se u obzir uzimaju samo direktni negativni efekti na pojedinca, ali ti efekti mogu imati uticaja i na druge. U slučaju da neki od članova zajednice na primer saznaju informacije koje drugi nisu, oni se na taj način ne samo izdvajaju u odnosu na druge već takođe mogu dovesti do diskriminacije ostalih. [4]

5. Mehanizmi za upravljanje privatnošću ličnih podataka

Najbolji način zaštite ličnih podataka je što manje ih otkrivati i činiti javno dostupnim. Mehanizmi koji mogu sprečiti zloupotrebu ličnih podataka su [4]: upravljanje parcijalnim identitetima, minimazacija podataka, izvršna pravila za obradu podataka i funkcionalna transparentnost.

Upravljanje parcijalnim identitetima i zaštita od zloupotrebe istih nisu trivijalni procesi. Lični podaci o pojedincu dostupni na personalnim računarima mogu biti ranjivi ako se računari ne koriste na pravilan način, i ako se ne vodi računa o bezbednosti samog sistema putem mnogobrojnih dostupnih zakrpa.

Minimizacija podataka ne odnosi se samo na količinu dostupnih informacija već i na smanjenu mogućnost identifikacije i povezivanja na osnovu dostupnih podataka. Komunikacija može biti enkriptovana i preusmerena na više različitih nezavisnih proksi servera koji garantuju anonimnost, osim ako sam korisnik ne otkrije neke od dodatnih informacija.

Ako lični podaci napuste okruženje koje kontroliše korisnik, on treba da bude obavešten o tome kao i o tome šta će se dalje sa tim podacima dešavati. Zakonskim propisima regulisana je mogućnost da se otkaže

saglasnost o obradi ličnih podataka. Problem se može javiti u slučaju da su se kopije podataka prenele na druge strane i tada se ne može izvšiti totalni opoziv.

Transparentnost je preduslov za sve vrste kontrole od strane korisnika. Informacije o sagovornicima u procesu komunikacije, njihovoj reputaciji, pouzdanosti ili nadležnostima koje imaju mogu biti vidljive korisniku, i predstavljati značajan faktor pre uspostavljanja komunikacionog odnosa.

6. Standardi upravljanja identitetima

Prilikom definisanja zahteva u fazi implementacije sistema za upravljanje identitetima potrebno je uraditi evaluaciju standarda. Razlikuju se standardi za Web servise (SOAP, USDL, UDDI), za sigurnost (SAML, WSS), za biometriju (BioAPI, CBEFF), itd. U nastavku rada definisani su neki od standarda.

SAML (*Security Access Markup Language*) predstavlja standard čiji je cilj sprovođenje rešenja koja se zasnivaju na autentifikaciji i autorizaciji u različitim sistemima upotrebom XML koda. SAML koristi Identity Provider (IdP) i Service Provider (SP) koncept. SP koncept se odnosi na treću stranu koja čuva informacije o drugom identitetu ili u ime drugog entiteta. [8][9]

Standard SPML (*Service Provisioning Markup Language*) namenjen je za upravljanje procesom primene korisničkih računa unutar različitih sistema. XACML (*eXtensible Access Control Markup Language*) je XML specifikacija za prenos i procesiranje podataka u sistemima koji se koriste za pristup informacijama putem Interneta.

WS-Security (*Web Service Security*) ima za cilj davanje podrške, integrisanje i standardizaciju različitih sigurnosnih modela, mehanizama i tehnologija koja će omogućavati interoperabilnost različitih sistema. XCBF (*eXtensible Common Biometric Format*) je standardna metoda prenosa biometrijskih identifikacionih podataka, kao što je skeniranje oka ili otisak prsta.

7. Upravljanje identitetima u oblaku

Razvoj koncepta Cloud sistema posmatran iz ugla različitih metodoloških pristupa, tehnoloških i poslovnih (SaaS, klaster sistemi, sistemi visokih performansi), ukazuje da se Cloud IDM može posmatrati kao sveobuhvatan pristup rešavanju svih problema iz ove oblasti, ali i šire. Cloud computing se definiše kao distribuiran računarski sistem, oblast unutar koje su klijentima na raspolaganju visoko skalabilni informaciono-komunikacioni kapaciteti. [10] Koncept Cloud computing-a bazira se na tehnologiji virtualizacije, koja predstavlja zamenu za fizičke računarske resurse. [11]

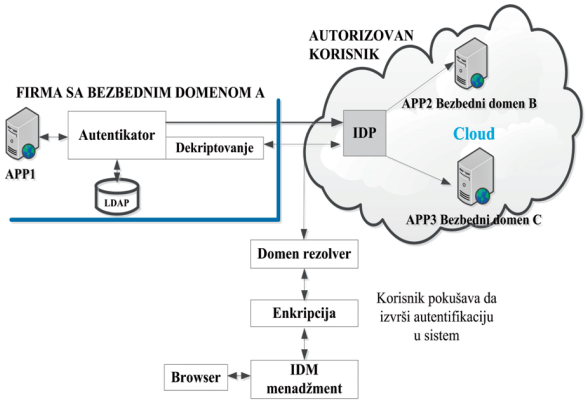
IDM u Cloud sistemu mora da upravlja: kontrolnim tačkama, dinamičkim zatvorenim sistemima, virtuelnim uređajima ili identitetima usluga. Implementacija Cloud sistema je dinamička sa serverima koji se pokreću ili se gase, IP adresama koje se dinamički dodeljuju i menjaju i servisima koji se pokreću, gase ili restartuju. Kada se uređaj ili servis gasi, IDM prima informaciju o tome kako bi ukinuo pristup instancama. IDM će detalje o pristupu instanci čuvati do trenutka do kada ona ponovo postane aktivna, a zatim će aktivirati i mehanizme autorizacije. Dok se pristup ponovo ne aktivira, detalji o pristupu moraju biti skladišteni i čuvani na odgovarajući i jasno definisan način. [8] [12]

Cloud sistemi zahtevaju promenu pristupa u odnosu na klasični IDM, posebno u delu koji se odnosi na omogućavanje, odnosno ukidanje pristupa, sinhronizaciju, dodelu privilegija, upravljanje životnim ciklusom identiteta, itd. Jedini način da se osigura bezbednost osetljivih podataka u Cloud sistemima za sada je šifrovanje. Jedno od najrasprostranjenih rešenja za šifrovanje podataka su PGP proizvodi koji nude šifrovanje na svakom mestu gde se podaci mogu nalaziti. Prednost PGP šifrovanja je u centralizovanom upravljanju proizvodima, što rasterećuje krajnje korisnike i oslobađa ih brige o ključevima ili odluke o tome kada je pravo vreme da se podaci šifruju. [13]

U Cloud sistemima razlikujemo tri IDM paterna [14]: Poverljivi IDM patern, Externi IDM patern i Interoperabilni IDM patern.

Poverljivi IDM patern namenjen je malim ili privatnim Cloud sistemima koji zahtevaju visok stepen sigurnosti. Stepen skalabilnosti je izuzetno nizak. Osnovna karakteristika ovog koncepta je da se autentifikacija uvek realizuje u okviru *firewall*-a. Autentifikacioni detalji se prosleđuju IDM komponenti, koja enkriptuje ove informacije i dalje, kroz bezbedan komunikacioni kanal, prosleđuje informaciju entitetu koji će realizovati autentifikaciju. IDM je nezavisan od autentifikacionog mehanizma, pa je implementacija i integracija ovog paterna brza i efikasna.

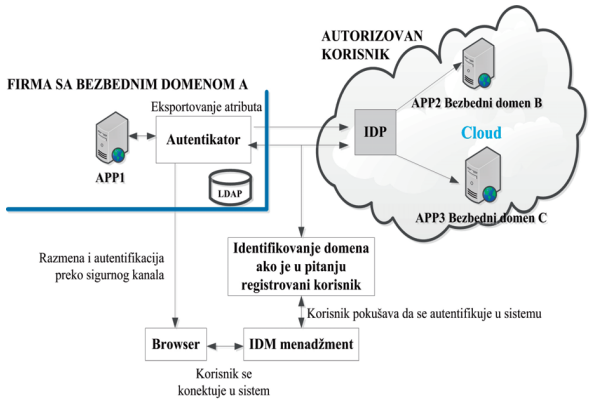
Nakon uspešne autentifikacije korisnika od strane bilo kog autentifikacionog mehanizma u Cloud sistemu, ostali serveri koji učestvuju u sistemu "veruju" tom korisniku. Atributi korisnika mogu biti deljeni konceptom, kao što je SAML, dok sama autorizacija može biti realizovana putem XACML-a. Primer je prikazan na Slici 3.



Slika 3 : Poverljivi IDM Patern [14]

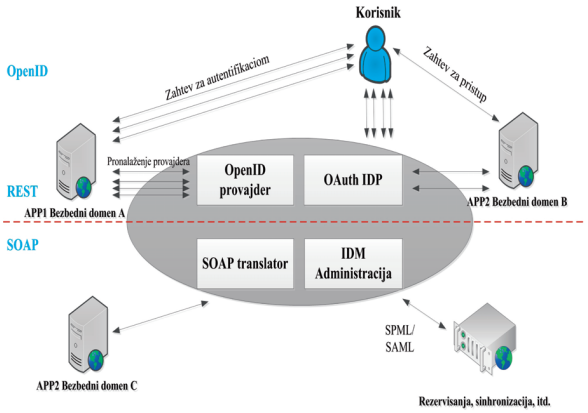
Externi IDM patern je sličan prethodnom, s tim što se autentifikacioni detalji direktno prosleđuju entitetu koji će realizovati autentifikaciju. Autentifikacioni detalji mogu biti prikupljeni pomoću različitih *browser*-a, a dostavljeni kanalom zaštićenim SSL-om.

Externi patern je namenjen javnim Cloud sistemima. IDM je posebno usmeren ka rešavanju pitanja domena i iniciranja procesa autentifikacije od strane entiteta koji će realizovati autentifikaciju. Arhitektonsko rešenje usvojeno je od strane Ping identiteta, gde se rešavanje pitanja domena realizuje referisanjem na odgovarajuću tabelu validnih korisnika, koja je uvek ažurna. Primer je prikazan na Slici 4.



Slika 4 : Eksterni IDM [14]

Interoperabilni IDM patern se koristi prilikom realizacije *Cloud2Cloud* komunikacije, korišćenjem OpenID i OAuth. OpenID je otvoreni i decentralizovani standard za autentifikaciju korisnika i kontrolu pristupa, koji omogućava da korisnici pristupaju različitim servisima ili serverima, sa istim digitalnim identitetom. OAuth je otvoreni protokol koji omogućava korisniku da drugom korisniku dodeli privilegiju pristupa lokaciji pružaoca usluge, bez deljenja autentifikacionih detalja. Ovo je izuzetno korisno za elektronsko poslovanje, gde različiti pružaoci usluge nude svoje proizvode/usluge na jednom mestu.



Slika 5: Interoperabilni IDM [14]

Uporedni prikaz sva tri IDM Cloud paterna prikazan je u Tabeli 1:

Tabela 1. Uporedni prikaz IDM Cloud paterna [14]

	Poverljivi IDM Patern	**Eksterni IDM**	**Interoperabilni IDM**
Bezbednost	Veoma bezbedan	Utvrđena IDP mreža	Zavisi od mehanizma autentifikacije
Interoperabilnost	Interoperabilan	Interoperabilan	Interoperabilan
Tip oblaka	Privatni oblak	Javni oblak	Javni oblak sa više tehnologija
Brzina implementacije	Veoma brz	Brz	Brzina zavisi od broja zahteva
Skalabilnost	Otežana skalabilnost	Otežana skalabilnost	Skalabilan
Primena	Google App Engine	Ping identitet	Predloženi dizajn

Zaključak

U radu su opisane osnove sistema za upravljanje identitetima, od opštih pojmova, pa do mehanizama i standarda za upravljanje identitetom. Cilj rada je prikaz koncepta digitalnih identiteta, kao osnove za implementaciju širokog spektra usluga u oblasti poslovanja na Internetu. Upravljanje identitetima je koncept duže vremena prisutan, ali je ubrzani razvoj elektronskog poslovanja proširio mogućnosti primene koncepta, pa su istraživanja u ovoj oblasti od šireg značaja kako za samo elektronsko poslovanje, tako i za prisustvo na Internetu uopšte. Internet okruženje i mnoštvo servisa koji su raspoloživi korisnicima doveli su do povećane potrebe da se u prvi plan stavi digitalni identitet entiteta. Digitalnim identitetima treba upravljati na strateški planiran, poslovno opravdan i kontrolisan način.

Upravljanje identitetom povlači i brojna sigurnosna pitanja. U trenutku kreiranja digitalnog identiteta, odnosno korišćenja određenih rešenja za upravljanje identitetima, otvara se mogućnost za realizaciju različitih nedozvoljenih i zlonamernih aktivnosti, pre svega u obliku krađe ili neovlašćenog preuzimanja digitalnog identiteta (eng. *identity theft*). Glavni zadatak upravljanja identitetima je da se pravi identitet koristi u pravom kontekstu u pravo vreme.

Primena Cloud sistema u realizaciji IDM koncepta treba da zadovolji zahteve koje postavlja Cloud sistem, kao i da ispuni uslove za buduća poboljšanja sistema. Primena ovog pristupa omogućiće da IDM koncept u odnosu na velike sisteme bude jednostavan, brz i efikasan, jer će se aktivnosti IDM-a realizovati u Cloud sistemu. Opisom upravljanja identitetom prikazane su prednosti i nedostaci ovog koncepta, dok se opisom elemenata sistema za upravljanje identitetom i metodologijom za implementaciju takvog sistema daje okvirni pregled koncepta, koji treba da posluži kao osnova za dalja istraživanja u ovoj oblasti.

LITERATURA

[1] Windley, P.J. Digital Identity, O'Reilly Media, Inc., Ch2, 2005.
[2] Harrop, M. Identity Management, The Cottingham Group, ETSI Security Workshop, 2009.
[3] Identity Management, The Government of the Hong Kong Special Administrative Region, 2008.
[4] Hansena, M., Pfitzmannb, A. and Steinbrecherb, S. Identity management throughout one's whole life, Information security technical report 13, pp. 83-94, 2008.
[5] Chawdhry, P. and Vakalis, I. Use of ePassport for Identity Management in Network-Based Citizen-Life Processes, Editor(s): Bezzi, M., Duquenoy, P., FischerHubner, S., Hansen, M. and Zhang, G., Privacy and Identity Management for Life, Book Series: IFIP Advances in Information and Communication Technology, Vol. 320, pp. 122-133, 2010.
[6] Glasser, U. and Vajihollahi, M. Identity Management Architecture, Simon Fraser University, Canada, 2008.
[7] Jin, Z.P., Xu, J., Xu, M. and Zheng, N. An Attribute-Oriented Model for Identity Management, International Conference on e-Education, e-Business, e-Management and e-Learning, 2010.
[8] Celesti, A., Tusa, F., Villari, M. and Puliafito, A. Security and cloud computing: Intercloud identity management infrastructure, 19th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2010, Larissa, pp. 263-265, 28-30 June 2010.
[9] Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Ben Othmane, L. and Lilien, L. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing, 29th IEEE Symposium on Reliable Distributed Systems 2010, New Delhi, pp. 177-183, 31Oct-3Nov 2010.
[10] Srinivasa, R., Nageswara, R. and Kusuma, K. Cloud Computing: An overview, Journal of Theoretical and Applied Information Technology, Vol. 9, No. 1, pp. 71-76, 2009.
[11] di Costanzo, A., de Assuncao, M.Di. and Buyya, R. Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure, IEEE Internet Computing, IEEE Computer Society, pp. 24-33, 2009.
[12] Sanchez, R., Almenares, F., Arias, P., Diaz-Sanchez, D. and Marin, A. Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing, IEEE Transactions On Consumer Electronics, Vol. 58, Issue 1, pp. 95-103, 2012.
[13] Vučinić, V. Sigurnost u oblacima, Internet ogledalo, No. 126-127, pp. 40-43, 2011.
[14] Gopalakrishnan, A. Cloud Computing Identity Management, SETLabs Briefings, Vol. 7, No. 7, pp. 45-53, 2009.

Primljen: Februar 2012.
Prihvaćen: Maj 2012.

O autoru

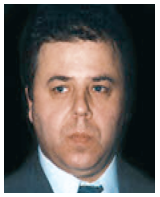
Marko Vulić
Fakultet organizacionih nauka u Beogradu, Stipendista Ministarstva za nauku i tehnološki tazvoj
e-mail: marko@elab.rs

Marko Vulić rođen je 1985. godine u Beogradu. Diplomske i Master studije završio je na Fakultetu organizacionih nauka u Beogradu. Trenutno je student druge godine doktorskih studija na FON-u, stipendista i član projektnog tima Ministarstva nauke i prosvete Republike Srbije. Oblasti naučnog interesovanja su: elektronsko poslovanje, mobilno poslovanje, Internet marketing, e-obrazovanje, e-bankarstvo, CRM. Kontakt:

Marko Ranković
EuroPlanet d.o.o, Beograd
e-mail: mrankovic@euronetworldwide.com

Oblasti profesionalnog interesovanja autora su upravljanje projektima u oblasti finansijskih servisa i usluga, naučno-istraživački rad u oblasti procesiranja elektronskih finansijskih transakcija, uključujući metode i tehnike procesiranja, organizacionu strukturu procesora, arhitekturu platforme za procesiranje transakcija, modele i tehnike zaštite sistem plaćanja platnim karticama. Marko R-anković je zaposlen u kompaniji EuroPlanet, na poslovima Project Manager-a.

Vojkan Vasković
Beogradska Poslovna Škola
e-mail: vaskovic@bvcom.net



Vojkan Vasković rođen je 1951. godine u Kragujevcu. Osnovne i poslediplomske (magistarske) studije završio je na Fakultetu organizacionih nauka u Beogradu gde je odbranio i doktorsku disetrtaciju. Zaposlen je kao profesor u Beogradskoj poslovnoj školi. Oblasti profesionalnog interesovanja su: elektronsko poslovanje, e-bankarstvo, Internet tehnologije, mobilne tehnologije, e-uprava.