HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Osnovni koncepti upravljanja digitalnim identitetima

CCERT-PUBDOC-2005-08-132

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Elektroničko poslovanje koje se temelji na pružanju usluga, u prvi plan stavlja digitalni identitet korisnika usluge te cjelokupni proces upravljanja digitalnim identitetima. Pojmovi anonimnosti i privatnosti, u suprotnosti su s provođenjem transakcija kojima se zahtjeva prodaja, kupovina ili pristup određenim servisima gdje je otkrivanje informacija o identitetu nužno.

Pojam digitalnog identiteta može se promatrati iz različitih perspektiva. Jedna od perspektiva jest perspektiva dobavljača programskih proizvoda koji služe za upravljanje identitetima, druga je perspektiva organizacija koje žele implementirati takva rješenja, a treća je perspektiva korisnika odnosno osobe čiji je digitalni identitet predmet upravljanja.

Upravljanje identitetom također povlači i brojna sigurnosna pitanja. Naime, u trenutku kreiranja digitalnog identiteta, odnosno korištenja konkretnih rješenja za upravljanje identitetima, otvara se mogućnost za provođenje različitih malicioznih aktivnosti, prvenstveno u obliku krađe ili neovlaštenog preuzimanja digitalnog identiteta (eng. *identity theft*). Glavna zadaća upravljanja identitetima jest da se pravi identitet koristi u pravom kontekstu u pravo vrijeme.

Dokument daje globalni pregled upravljanja digitalnim identitetima, uzimajući pri tom u obzir spomenute aspekte. U poglavlju o općim pojmovima analizirane su osnovni elementi te način rada sustava. Opisom upravljanja identitetom općenito se ističu zahtjevi te prednosti i nedostaci ovog koncepta, dok se opisom elemenata sustava za upravljanje identitetom te metodologijom za implementaciju takvog sustava daje se okvirni pregled koncepta. Dodatne informacije o standardima upućuju na različite funkcije o kojima treba voditi računa pri upravljanju identitetom. Načini krađe identiteta opisani su informativno radi podizanja svijesti.

Općenito govoreći, pojmovi upravljanja identitetima, odnosno digitalnih identiteta imaju široko značenje, pa je u ovom dokumentu dat generalni pregled osnovnih značajki.

2. Definiranje općih pojmova

Za razumijevanje koncepta upravljanja digitalnim identitetima potrebno je prije svega definirati neke osnovne pojmove:

- subjekt, entitet (engl. *subject*, *entity*),
- resurs (engl. *resource*),
- identitet (engl. *identity*),
- atribut (engl. *attribut*),
- sklonost (engl. *preference*),
- značajka (engl. *trait*),
- identifikacijski podaci (engl. *credentials*),
- sigurnosni autoritet (engl. *security authority*),
- upravljanje digitalnim identitetom (engl. *identity management*).

Subjekt ili entitet je osoba, grupa ljudi, organizacija, programski alat ili bilo koji drugi entitet koji zahtjeva pristup određenom resursu.

Resurs može biti Web stranica, podatak u bazi podataka, transakcija kreditnom karticom, i sl. Ono što je osnova pristupa resursu jest da se subjekt prilikom ostvarivanja pristupa poziva na svoj digitalni identitet.

Identitet jest skupina podataka koji prezentiraju atribute, sklonosti i značajke subjekta. Jednom riječju, identitetom se smatra skup informacija koji je poznat o određenom entitetu.

Atributima subjekta smatraju se informacije kao što su godine, zdravstveni podaci, podaci o navikama naručivanja putem Interneta, kreditna sposobnost, itd.

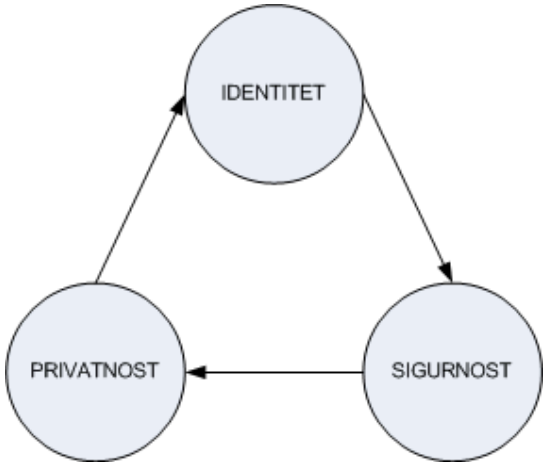
Sklonosti podrazumijevaju podatke o tome što korisnik preferira od prijevoznih sredstava, vrste hrane i sl.

Značajke su svojstva korisnika koja su nasljedna kao npr. boja očiju, i sl.

Subjekt potvrđuje svoj identitet radi pristupa resursu putem uvjerenja. Identifikacijski podaci predstavljaju dokaz da određeni subjekt odgovara identitetu za koji se izdaje.

Identifikacijski podaci se prezentiraju sigurnosnom autoritetu koji ih mora autenticirati. Autentikacija se može izvesti uporabom korisničkog imena i zaporke, pomoću X.509 certifikata ili

biometrije. Ovisno o tome koji je potencijali rizik za određeni resurs te vrijednost resursa, uvode se različite tehnike autentikacije.
Kada se potvrdi autentičnost uvjerenja, sigurnosni autoritet uspostavlja sigurnosnu politiku za resurs. Sigurnosna politika služi za dokazivanje da odgovarajući identitet ima određena prava i dozvole nad odgovarajućim resursom.
Uz pojam identiteta usko se povezuju i pojmovi sigurnosti i privatnosti. Informacijska sigurnost područje je koje se bavi zaštitom integriteta, tajnosti i povjerljivosti informacija. Privatnost je zaštita atributa, sklonosti i značajki pri svakoj transakciji koju entitet učini.
Veza između navedena tri pojma prikazana je na slici Slika 1.



Slika 1: Odnos identiteta, sigurnosti i privatnosti

Upravljanje digitalnim identitetima definira se kao proces kojim se postojeće tehnologije koriste za upravljanje informacijama o digitalnom identitetu entiteta te za kontrolu pristupa resursima. Cilj upravljanja digitalnim identitetima jest poboljšanje produktivnosti i sigurnosti uz smanjenje troškova povezanih s upravljanjem entitetima i njihovim digitalnim identitetima.
Za upravljanje identitetom postoje razni termini i akronimi kao što su:

- upravljanje identitetom (engl. *Identity Management*)– IM, IdM, IDM,
- upravljanje identitetom i pristupom (engl. *Identity and Access Management*) – IAM,
- sigurno upravljanje identitetom (engl. *Secure Identity Management*) – SIM,
- digitalni identitet (engl. *Digital Identity*) – DI, DID,
- upravljanje identitetom i sigurnošću (engl. *Identity and Security Management*) – ISM.

Zbog jednostavnosti, u daljnjem tekstu će se koristiti pojmovi identitet i upravljanje identitetima.

3. Upravljanje identitetima

Upravljanje identitetima koristi se u svakodnevnom životu. Entitet (osoba) kroz različite komunikacijske kanale pruža svom sugovorniku određeni skup informacija o sebi, a taj skup informacija se mijenja ovisno o kontekstu. Kao što je već spomenuto, glavna zadaća upravljanja identitetima jest da se identitet koristi u pravom kontekstu u pravo vrijeme.
U kontekstu digitalnog identiteta, upravljanje identitetima uglavnom se promatra kao koncept za:

- definiranje identiteta entiteta,
- spremanje relevantnih informacija o entitetu na siguran i fleksibilan način,
- omogućavanje pristupa informacijama putem definiranog sučelja,
- osiguranje fleksibilne, distribuirane i kvalitetne infrastrukture za upravljanje identitetima.

Ovaj koncept obuhvaća četiri glavna pojma povezana s upravljanjem identitetom:

1. autentikaciju,
2. autorizaciju,
3. kontrolu pristupa,
4. nadzor.

Autentikacija je proces provjere identiteta entiteta koji ima za cilj potvrditi da je entitet upravo onaj za koji se isti izdaje. Postoji nekoliko metoda autentikacije, a dijele se na tri glavne skupine:

- nešto što entitet zna (npr. korisničko ime i zaporka),
- nešto što entitet ima (npr. token),
- nešto što entitet jest (npr. skeniranje otiska prsta).

Autorizacija je proces u kojem se entitetu odobrava pristup resursima nakon što je uspješno završen proces autentikacije.
Kontrola pristupa može se opisati kao skup politika koje definiraju pravila korisničkog računa.
Nadzor obuhvaća izvješća o upravljanju identitetu te kontrolu.

3.1. Zahtjevi upravljanja identitetima

Upravljanje identitetima, osim spomenutih ciljeva, ima zadaću omogućiti različitim servisima korištenje istih korisničkih informacija. Zahtjevi koji tom prilikom trebaju biti zadovoljeni su:

- funkcionalnost i
- privatnost.

Funkcionalnost ovog sustava ogleda se kroz kreiranje, spremanje te pristupanje identitetima pa je to ujedno i prvi zahtjev koji mora biti zadovoljen.
Privatnost se očituje kroz dva aspekta. Prvi aspekt jest da identitet entiteta nije dostupan ostalim entitetima ukoliko osoba to nije odobrila. Drugi aspekt jest da podaci koje treća osoba posjeduje o entitetu moraju biti na raspolaganju određenom stupnju kontrole od strane samog entiteta.

3.2. Prednosti i nedostaci upravljanja identitetima

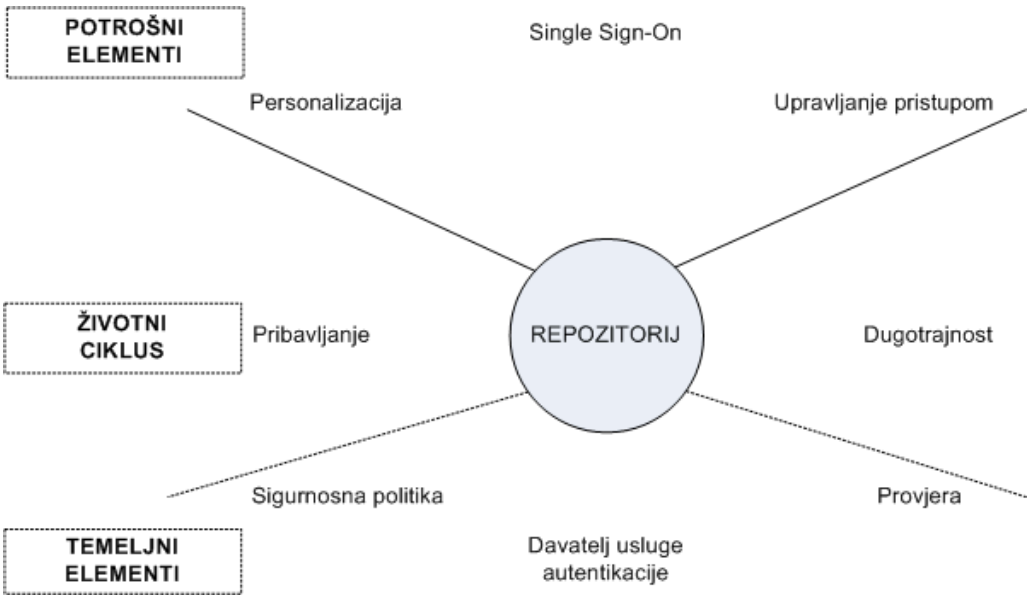
Organizacije koje uspostave sustav upravljanja identitetima imaju mnoštvo prednosti, a neke su:

- smanjenje troškova uvođenja svih sustava,
- smanjenje nepotrebnih kadrova,
- optimizacija poslovnih procesa,
- poboljšanje usluga za klijente i zaposlenike te osiguranje kontrole i privatnosti klijenata, dobavljača i zaposlenika,
- smanjenje vremena potrebnog za dobivanje pristupa potrebnim resursima unutar organizacije,
- smanjenje rizika posjedovanja netočnih informacija koje se koriste u poslovnim procesima,
- smanjenje rizika od strane bivših zaposlenika koji pokušavaju pristupiti organizacijskim resursima,
- podržavanje pravnih pitanja povezanih sa zaposlenicima i klijentima (npr. European Data Protective Directive).

Osnovni nedostatak pri upravljanju identitetima jest nekompatibilnost različitih tehnologija namijenjenih upravljanju identitetima. Trenutna situacija na tržištu, među tvrtkama, jest da su izolirane, neovisne te ne komuniciraju niti vjeruju jedna drugoj. To rezultira različitim aplikacijama s vlastitim načinom pohrane i upravljanja identitetima. Za korisnika taj nedostatak izaziva mnogostruke prijave u različite sustave, pamćenje više korisničkih imena i zaporki, upotrebu nekoliko vrsta kartica, tokena i ostalih tehnologija koje služe za autentikaciju.

4. Elementi sustava za upravljanje identitetima

Rješenja za upravljanje identitetima su modularna i sastavljena od više servisa i sistemskih komponenti. Primjer jedne strukture za upravljanje identitetima s pripadajućim komponentama prikazan je na slici (Slika 2).



Slika 2: Elementi sustava za upravljanje identitetom

Elementi su raspoređeni u tri skupine. To su:

1. temeljni elementi (engl. *foundation*),
2. elementi životnog ciklusa (engl. *lifecycle*),
3. potrošni elementi (engl. *consumable*).

4.1. Repozitorij

Repozitorij (engl. *repository*) predstavlja jezgru sustava za upravljanje identitetom. Repozitorij je centralno mjesto za pohranu logičkih podataka i identiteta koji je obično implementiran u obliku LDAP (*Lightweight Directory Access Protocol*) imenika ili meta-direktorija. Pristup direktoriju i svim informacijama ograničava se primjenom sigurnosne politike koja je također pohranjena unutar repozitorija.

4.2. Davatelj usluge autentikacije

Davatelj usluge autentikacije (engl. *authentication provider*) naziva se još i davatelj identiteta (engl. *identity provider*), a odgovoran je za provođenje primarne autentikacije entiteta koja se odnosi na uspostavljanje veze između entiteta i identiteta. Davatelj usluge kreira autentikator – token koji omogućuje ostalim komponentama prepoznavanje provođenja procesa autentikacije. Primarna autentikacija obuhvaća autentikacijske tehnike kao što su korisničko ime i zaporka, token, pametne kartice (engl. *smartcard*), biometrija ili X.509 certifikati. Jedan identitet može biti pridružen jednom ili nekolicini davatelja usluge autentikacije.

4.3. Sigurnosna politika

Pristup i korištenje informacija o identitetu vođeno je kontrolama sigurnosne politike. Sigurnosna politika određuje način na koji će se manipulirati informacijama.

4.4. Provjera

Provjera (engl. *auditing*) predstavlja mehanizam kojim se prati način na koji se informacije u repozitoriju kreiraju, modificiraju i koriste. Ovaj mehanizam čini osnovu za forenzičnu analizu ukoliko je potrebno utvrditi tko i na koji način je zaobišao kontrole.

4.5. Pribavljanje identiteta

Pribavljanje identiteta (engl. *provisioning*) jest postupak automatizacije svih procedura i alata koji čine životni ciklus identiteta. Tu spadaju:

1. kreiranje identifikatora identiteta,
2. povezivanje s davateljem usluge autentikacije,
3. podešavanje i promjena atributa i ovlasti,
4. onemogućavanje identiteta.

4.6. Dugotrajnost

Alati koji omogućuju dugotrajnost identiteta (engl. *longevity*) ujedno kreiranju i zapise o povijesti identiteta. Oni omogućuju ispitivanje evolucije identiteta tijekom određenog perioda vremena.

4.7. Single Sign-On

Single Sing-On (SSO) koncept omogućuje korisniku da se samo jednom prijavi u sustav i da nakon toga ima omogućen pristup svim aplikacijama i servisima koji čine dio okruženja njegovog identiteta. Najpoznatiji protokol kojim se implementira SSO funkcionalnost je Kerberos, koji se između ostaloga koristi i kao autentikacijski protokol kod Windows operacijskih sustava.

4.8. Personalizacija

Personalizacija (engl. *personalization*) jest značajka upravljanja identitetima gdje se specifične aplikacije i generičke informacije pripisuju identitetu. Personalizacija jest tehnika kojom se servisi prilagođavaju ponaosob svakom korisniku. Personalizacija se temelji na filtriranju informacija o servisu korištenjem informacija o korisniku (profil).

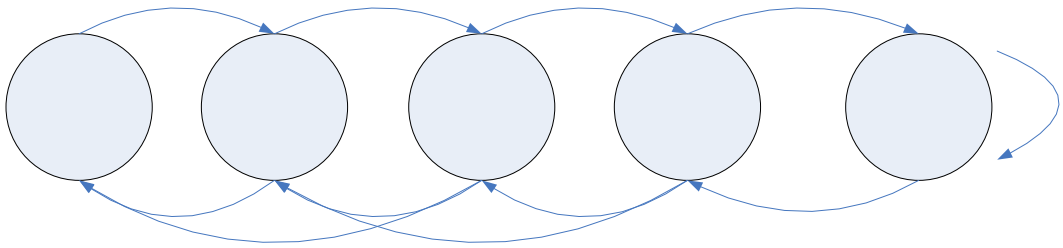
4.9. Upravljanje pristupom

Upravljanje pristupom (engl. *access managmenet*) omogućava da se kreiranjem jasnog i jedinstvenog identiteta za svaki pojedini entitet pojednostavi i racionalizira kontekst korištenja identiteta te da se definiraju sigurnosne politike temeljene na profilu. Na taj način olakšano je upravljanje pristupom resursima.

5. Implementacija sustava za upravljanje identitetima

Implementacija sustava za upravljanje identitetima odvija uglavnom nadogradnjom na postojeću sigurnosnu infrastrukturu te čini još jednu sigurnosnu komponentu cjelokupnog sustava. Iako je implementacija usko povezana sa sigurnosnim zahtjevima, potrebno je naglasiti da ovaj proces treba biti na višoj razini te zadovoljiti poslovne zahtjeve.

Za pravilnu implementaciju potrebno je napraviti strateški plan, a zatim i plan tehničke implementacije sustava. Definiranje strategije upravljanja identitetima primaran je proces svake organizacije. Strategija podrazumijeva dugoročni plan koji će sadržavati način na koji će se informacije o identitetu koristiti u poslovanju, uzimajući u obzir korisnike identiteta: partnere, klijente i zaposlenike. Plan implementacije sastoji se od pet faza prikazanih na slici Slika 3.



Slika 3: Faze implementacije sustava za upravljanje identitetima

Proces sastavljen od prikazanih faza čini metodologiju implementacije sustava za upravljanje identitetima.

Definiranje (engl. *define*) podrazumijeva određivanje opsega i krajnjih rezultata koji se žele postići u organizacijskom okruženju. Ovaj korak osigurava organizaciji definiranje željene funkcionalnosti, postavljanje prioriteta te postavljanje kriterija za izbor krajnjeg proizvoda za upravljanje identitetima.

Dizajn (engl. *design*) je faza u kojoj se postavljaju detalji krajnjih rezultata koji se žele postići, dokumentiranje i kreiranje plana implementacije na višoj razini.

Razvoj (engl. *develop*) sustava znači kreiranje koda odnosno izbor alata koji zadovoljava postavljene kriterije organizacije kao i detaljan projektni plan implementacije. U ovoj fazi planira se i testiranje rješenja tijekom kojeg se uspoređuje koliko testirano rješenje zadovoljava potrebe organizacije definirane u ranijim fazama.

Puštanje u rad (engl. *deploy*) je faza u kojoj se rješenje isporučuje.

Podrška (engl. *sustain*) je faza u kojoj se izrađuje i provodi plan podržavanja i održavanja implementiranog sustava tijekom njegova životnog ciklusa.

U praksi nema jedinstvenog pristupa implementaciji. Ne postoji jedinstveno rješenje, već organizacije trebaju definirati svoje zahtjeve temeljene na poslovnoj strategiji.

6. Standardi upravljanja identitetima

Standardi upravljanja identitetima trebaju se evaluirati prilikom definiranja zahtjeva u prvoj fazi implementacije sustava za upravljanje identitetima. Obično se dijele po funkcijama pa tako razlikujemo standarde za Web servise (SOAP, USDL, UDDI), standarde za sigurnost (SAML, WSS), standarde za biometriju (BioAPI, CBEFF), itd. U nastavku su navedeni i opisani samo neki od standarda.

SAML (*Security Access Markup Language*) je standard koji ima za cilj provoditi rješenja temeljena na sekcijama za autentikaciju i autorizaciju unutar nejednakih sustava upotrebom XML izraza. Ovaj standard dizajniran je s ciljem razmjene informacija između različitih sustava web servisa.

SPML (*Service Provisioning Markup Language*) je standard za upravljanje procesom primjene korisničkih računa unutar različitih sustava.

XACML (*eXtensible Access Control Markup Language*) je XML specifikacija za prijenos i primjenjivanje podataka iz politika za pristup informacijama putem Interneta. Cilj ovog standarda je definirati pravila koja specificiraju tko, što, kada i kako treba imati pristup informacijama.

WS-Security (*Web Service Security*) ima za cilj davati podršku, integrirati i unificirati mnoštvo sigurnosnih modela, mehanizama i tehnologija koja će omogućavati interoperabilnost različitim sustavima. WS-Security specifikacija definira skup standarda SOAP (*Simple Object Access Protocol*) koji omogućuju implementaciju integriteta i povjerljivosti u web servise. Ovo je standardna metoda kojom se sigurnosni podaci dodaju poruci web servisa.

XCBF (*eXtensible Common Biometric Format*) je standardna metoda prijenosa biometrijskih identifikacijskih podataka kao što je skeniranje retine ili otisak prsta.

7. Krađa identiteta

Krađa identiteta sve je učestaliji zločin. Uobičajeni scenariji kojima se zlonamjernici služe su:

- kopanje po smeću (engl. *dumpster diving*),
- krađa poruka elektroničke pošte (engl. *mail theft*),
- krađa osobnih stvari (engl. *personal property theft*),
- unutarnji izvori (engl. *inside sources*),
- varalice (engl. *impostors*),
- *online* aktivnosti (engl. *online activities*).

U prvom scenariju, koliko god to nevjerojatno zvučalo običnom korisniku, kradljivci identiteta čeprkaju po smeću tražeći dijelove raskomadanih informacija koje mogu upotrijebiti ili čak prodati. Dokumenti koji sadrže informacije koje mogu poslužiti kradljivcima su računi kreditnih kartica, telefona, struje, itd., omotnice pristigle pošte pa i dokumenti o članstvu koji sadrže osobne podatke. Prilikom odlaganja ovakve vrste informacija treba izričito voditi računa o tome da se, prije odlaganja u smeće, takvi dokumenti pravilno uništeni (engl. *shred*).

Pretraživanje poštanskih sandučića i krađa poruka elektroničke pošte je scenarij u kojem kradljivci dolaze do informacija prije samog korisnika. Bilo kakva poruka elektroničke pošte koja sadrži podatke o financijskim transakcijama, poreznim obrascima ili sličnim informacijama koje se mogu iskoristiti i omogućuju krađu identiteta zanimljiva je ovoj vrsti ljudi.
Krađa osobnih stvari još je jedan od scenarija kako je lako doći do identiteta. Najjednostavniji primjer jest krađa novčanika u kojem se uobičajeno nalaze svi identifikacijski dokumenti, kreditne kartice pa i članske iskaznice. Međutim, i krađa prijenosnih računala, planera, te aktovki može biti izvor korisnih informacija za kradljivce.
Rastući trend u krađi identiteta jest posredovanje informacijama od strane unutarnjih izvora informacija. Nezadovoljan ili nelojalan zaposlenik koji ima pristup osobnim informacijama, ukoliko se odluči na takav korak, može prodati informacije onima koje su te informacije potencijalno zanimljive ili korisne.
Varanje je još jedan uobičajeni oblik krađe identiteta gdje se koriste bilo kakve prijevare kako bi se od žrtve izvukle osobne informacije.
Online aktivnosti uvelike povećavaju otkrivanje osobnih informacija. Unosom osobnih podataka putem formi na web stranicama te ostalim transakcijama koje korisnik obavlja *online* ostavlja se mogućnost za krađu identiteta korisnika.

8. Zaključak

Digitalno okruženje i mnoštvo servisa koji su korisnicima stavljeni na raspolaganje doveli su do povećane potrebe da se u prvi plan stavi digitalni identitet entiteta. Digitalnim identitetima treba upravljati na strateški planiran, poslovno opravdan i kontroliran način.
U dokumentu su opisane osnovne značajke sustava za upravljanje identitetima od općih pojmova pa do scenarija krađe identiteta. Cilj dokumenta bio je upoznati široku publiku s konceptom upravljanja identiteta te staviti naglasak na širinu koncepta, problematiku o kojoj treba razmišljati prije implementacije te spomenuti široku paletu standarda koji se razlikuju po funkcijama.
Upravljanje identitetima jest koncept koji je duže vremena prisutan, ali je sve popularnije elektroničko poslovanje proširilo koncept te je svakako preporučljivo daljnje informiranje o digitalnom identitetima te upravljanju identitetima općenito.

9. Reference

[1] Windley, J. P.: Understanding Digital Identity Management
www.windley.com/docs/Digital%20Identity.pdf

[2] Pato, J.: Identity Management: Setting Context
http://scholar.google.com/url?sa=U&q=http://www.hpl.hp.com/techreports/2003/HPL-2003-72.pdf

[3] Reed, A.: The Definitive Guide to Identity Management
http://searchcio.techtarget.com/searchCIO/downloads/DGIM_Ch1Excerpt.pdf

[4] Lee, C. S.: An introduction to Identity Management
http://www.giac.org/certified_professionals/practicals/gsec/2646.php

[5] Koch, M.; Worndl, W.: Community Support and Identity Management
http://scholar.google.com/url?sa=U&q=http://www11.in.tum.de/publications/pdf/Koch2001a.pdf

[6] Koch, M.: Global Identity Management to Boost Personalization
http://scholar.google.com/url?sa=U&q=http://www11.in.tum.de/publications/pdf/Koch2002f.pdf