DOI: 10.19279/TVZ.PD.2016-4-2-12

SIGURNOSNE TEHNOLOGIJE ZAŠTITE DOKUMENATA DOCUMENT SECURITY TECHNOLOGIES

Jana Žiljak Vujić[1], Ljiljana Matuško Antonić[2], Slaven Crnjac[1]

[1]Tehničko veleučilište u Zagrebu
[2]Općinski građanski sud u Zagrebu

Sažetak

Današnje vrijeme predstavlja nove izazove u zaštiti identiteta osoba kao i zaštiti vrijednosti pravnih i fizičkih osoba. Velike migracije stanovništva uzrokovane sukobima i ekonomskim poteškoćama predstavljaju veliki rizik prema krađi identiteta dok sve viša izloženost cyber napadima predstavlja veliki problem za državnu upravu te za pravne osobe kojima neovlašteni pristup ili krađa podataka čini veliki materijalni i nematerijalni gubitak. Uporabom samo e-pristupa određenim uslugama ili servisima, izlažemo se velikom riziku. Stoga se čini pravi način da ključne dokumente i isprave pokušamo zaštiti uporabom višestrukih zaštita, što grafičkih, što informatičkih, te uparujući zaštitu ispisa dokumenta(isprave) sa online bazama istih. U ovom članku opisati će se prednosti upotrebe višestruke zaštite dokumenata.

Ključne riječi: *zaštita dokumenata, cyber napadi, krađa identiteta, aktivna zaštita dokumenata, pasivna zaštita dokumenata, infrared, sigurnosne tehnologije zaštite ispisa.*

Abstract

Today's era poses new challenges to protect the identity of persons and protect the value of companies and individuals. Large migration of population caused by conflicts and economic difficulties represent a major risk to identity theft while all higher exposure to cyber attacks is a major problem for public administration and for legal entities to which unauthorized access or stealing information makes it a great material and immaterial losses.
Using only e-access to certain benefits and services, we are in big risk. Therefore, it seems the right way to protect essential documents and papers using of multiple protection and pairing protect printed documents with online database at the same time. This article will describe the benefits of using multiple technologies of document protection.

Keywords: document protection, cyber attacks, identity theft, active document protection, passive document protection, infrared, document security technologies

1. Uvod

1. *Introduction*

Ubrzani tržišni odnosi ne svode se samo u granice jedne države već iziskuju proširenje poslovanje na međunarodna tržišta radi povećanja dobiti, a što je jedan od temeljnih ciljeva pravnih subjekata. Migracije stanovništva, poslovanje na međunarodnom tržištu te obavljanje raznih pravnih poslova fizičkih osoba zahtijevaju dostupnost podataka na efikasan način. Kako bi se podaci učinili dostupnim sve većem broju korisnika službeni dokumenti pravnih osoba kao i osobni podaci o fizičkim osobama te njihovoj imovini ne vode se samo u analognom obliku već sve više i u digitalnom obliku. Dostupnost službenih dokumenata putem interneta olakšava poslovanje pravnih subjekata, ali i fizičkih osobama koje na brži i efikasniji način mogu izvršiti uvid u službene podatke javnih i državnih ustanova koje takve podatke vode u elektroničkom obliku.
Imajući u vidu da tijela državne uprave i javnih ustanova svoje poslovanje čine efikasnijim vođenjem podataka u digitalnom obliku postavljamo pitanje zaštite takvih podataka u pravnom prometu. Zaštita službenih dokumenata i osobnih podataka fizičkih osoba koje se vode u

digitalnom obliku i koje su dostupni većem broju osoba putem interneta predstavlja jedan od većih izazova na području informatike.

2. Pravni aspekt problema zaštite podataka

2.1 *Zakonodavni okvir u Republici Hrvatskoj*

Republika Hrvatska kao članica Vijeća Europe potpisnica je Konvencije o zaštiti osoba glede automatske obrade osobnih podataka (Konvencija 108) i Dodatnog protokola uz Konvenciju 108 u vezi nadzornih tijela i međunarodne razmjene podataka. Primjena odredbi navedenih akata Vijeća Europe omogućena je donošenjem Zakona o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.[1]

Temeljni zakonodavni okvir za zaštitu podataka u Republici Hrvatskoj nalazimo u Ustavu Republike Hrvatske, Zakonu o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka i Zakonu o potvrđivanju izmjena i dopuna Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (ETS br. 108) koje Europskim zajednicama omogućavaju pristupanje. Nadalje zaštita podataka sadržana je i u Zakon o zaštiti osobnih podataka, Uredbi o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka[2] i Uredbi o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka.[3]

Člankom 37. Ustava Republike Hrvatske propisano je da se svakom jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Nadalje čl. 37. Ustava Republike Hrvatske propisuje da se zakonom uređuje zaštita osobnih podataka te nadzor nad djelovanjem informatičkih sustava u državi te je zabranjena uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.

Temeljem ustavne odredbe o pravu na zaštitu osobnih podataka donesen je Zakon o zaštiti osobnih podataka. Zakon o zaštiti osobnih podataka, kao temeljni akt u području zaštite osobnih podataka u RH također je u svim bitnim odredbama sukladan Direktivi 95/46/EZ o zaštiti pojedinaca glede obrade osobnih podataka i o slobodnom kretanju takvih podataka. Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o zaštiti osobnih podataka. Agencija obavlja sljedeće poslove kao javne ovlasti: nadzire provođenje zaštite osobnih podataka; ukazuje na uočene zloupotrebe prikupljanja osobnih podataka; rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom; vodi središnji registar.

Kao podzakonski akti u području zaštite osobnih podataka u RH u primjeni su Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka. Zakon o zaštiti osobnih podaaka uređuje zaštitu osobnih podataka fizičkih osoba i nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u RH. Odredbom članka 1. Zakona o zaštiti osobnih podataka propisano je da se Zakonom uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama. Odredbe Zakona o zaštiti podataka primjenjuju se na obradu osobnih podataka od strane državnih tijela, tijela lokalne i područne (regionalne) samouprave te pravnih i fizičkih osoba, predstavništava i podružnica stranih

1 "Narodne novine" broj 04/05, Međunarodni ugovori
2 „Narodne novine" broj 105/2004
3 „Narodne novine" broj 139/2004

pravnih osoba i predstavnika stranih pravnih i fizičkih osoba koje obrađuju osobne podatke. Osobni podaci u zbirkama osobnih podataka moraju biti odgovarajuće zaštićeni od slučajne ili namjerne zlouporabe, uništenja, gubitka, neovlaštenih promjena ili dostupa (čl. 18. Zakona). Voditelj zbirke osobnih podataka i korisnik dužni su poduzeti tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka koje su potrebne da bi se osobni podaci zaštitili od slučajnog gubitka ili uništenja i od nedopuštenog pristupa, nedopuštene promjene, nedopuštenog objavljivanja i svake druge zlouporabe te utvrditi obvezu osoba koje su zaposlene u obradi podataka, na potpisivanje izjave o povjerljivosti. Svaka osoba koja smatra da joj je povrijeđeno neko pravo zajamčeno Zakonom o zaštiti podataka može podnijeti zahtjev za utvrđivanje povrede prava Agenciji za zaštitu osobnih podataka.

2.2 E-građani

2.2 *E-citizens*

Vlada Republike Hrvatske pokrenula je projekt e-Građani **Odlukom o pokretanju projekta e-Građani**[4] kojem je prvenstveno cilj modernizacija i ubrzanje komunikacije između građana i javne uprave, ali i povećanja transparentnosti javnog sektora u pružanju javnih usluga putem Središnjeg državnog portala koji objedinjava informacije o radu Vlade i ministarstava, informacije o javnim uslugama te omogućava siguran pristup elektroničkim uslugama. Sustav je uspostavljen kako bi tijela javnog sektora putem odgovarajuće web aplikacije i web servisa komunicirala s javnošću te sa svojim korisnicima, primjerice, radi objave javnih informacija i/ili slanja osobnih službenih poruka korisnicima vezanih za javne usluge, postupke i osobne statuse.
Projektom Vlade Republike Hrvatske e-Građani želi se omogućiti komunikacija građana s javnim sektorom na jednom mjestu na internetu, putem portala koji će objediniti informacije o radu Vlade i ministarstava, informacije o javnim uslugama te omogućiti siguran pristup elektroničkim uslugama korištenjem elektroničkog identiteta posredstvom jedne ili više prihvatljivih vjerodajnica za elektroničku identifikaciju (npr. korisničko ime/zaporka, token, digitalni certifikat i sl.). Projektom su obuhvaćene i elektroničke usluge - javne usluge koje državna tijela i javne službe pružaju krajnjim korisnicima putem interneta. Glavni cilj koji se žele postići Projektom e-Građani je omogućavanje što većeg broja elektroničkih usluga na višim razinama informatiziranosti.
Uspostavom centralnog internetskog rješenja za informacije (Središnji državni portal) građani mogu mnogo jednostavnije pronaći, recimo, podatke o promjeni osobnih dokumenata ili upisima u srednju školu. **Informacije se mogu tražiti pomoću ključnih riječi, po tipu ili temi**. Putem Osobnog korisničkog pretinca, među inim mogu se zatražiti elektronički izvodi iz matične knjige rođenih, vjenčanih ili knjige državljana, zatražiti elektroničke zapise uvjerenja o prebivalištu, boravištu te vlasništvu cestovnih vozila, informirati se o ocjenama djeteta u školi, pretraživati osnovne katastarske podatke i podnositi zahtjeve za izdavanje javnih isprava i rješavanje katastarskim uredima. U osobni korisnički pretinac mogu se zaprimati poruke i obavijesti o isteku osobne iskaznice, putovnice, vozačke dozvole ili registracije vozila, pravima iz mirovinskog i zdravstvenog osiguranja, obračunatom porezu na dohodak.
U pravnom sustavu Republike Hrvatske donesen je niz zakonskih i podzakonskih akata kojim se propisuju postupci za izradu zaštićenih isprava i službenih obrazaca i vezano za izdavanje, tiskanje i prodaju zaštićenih službenih obrazaca te ostalih službenih obrazaca čiji su sadržaj, oblik, način zaštite i obvezna primjena propisani zakonima, drugim propisima i aktima, a koji se objavljuju u "Narodnim novinama" koje su službeno glasilo Republike Hrvatske.[5]

2.2.1 Kaznena djela krivotvorenja službenih isprava

2.2.1 *Criminal offenses of counterfeiting official documents*

Razvoj i uporaba suvremenih tehnologija postavlja nove izazove jer je neophodno

4 "Narodne novine" broj 52/2013 i 31/2014

5 Primjerice Odluka o ispravama i službenim obrascima čiji su sadržaj, oblik, način zaštite i obvezna primjena propisani zakonima i drugim propisima (Narodne novine, br. 50/2011, 119/2011, 28/2013, 96/2013, 47/2014 i 61/2015) te Izmjene i dopune Popisa isprava i službenih obrazaca u 2014.

zaštiti osobne podatke koji se vode u zbirkama osobnih podataka, a koji podaci su dostupni putem interneta većem broju osoba. Nadalje svakodnevno podnošenje zahtjeva tijelima javne i državne uprave (primjerice potvrde o nekažnjavanju, podnošenje zahtjeva za izdavanje osobnih iskaznica i/ili putovnica, zahtjevi za promjenu adrese stanovanja i slično) te izdavanje raznih potvrda i službenih isprava u elektroničkom obliku omogućilo bi efikasniji rad tijela državne i javne uprave, ali bi omogućilo i građanima da takve poslove obavljaju na brži način uz manje potrošenog vremena po uredima državne i javne uprave. Građani se svakodnevno susreću sa zahtjevima za predajom dokumenata primjerice kod zapošljavanja trebaju predati dokaze o svojoj stručnoj spremi, potvrde o nekažnjavanju, domovnice i drugo. Prikupljanje dokumenata iziskuje odvajanje vremena kako bi se osobnim odlaskom u nadležne urede ishodili potrebni dokumenti.

Javne isprave kojima se služimo u pravnom prometu, a neke se pojedine javne isprave mogu ishoditi putem interneta, podložne su krivotvorenju. Na žalost susrećemo se i zlouporabom osobnih podataka u pravnom prometu radi postizanja određene imovinske koristi. Isto tako nije nepoznat slučaj krivotvorenja diploma, odnosno potvrda o stručnoj spremi koje se predaju uz zamolbu za natječaj za određena radna mjesta u javnoj i državnoj upravi kao i kod zapošljavanja kod privatnih poslodavaca, krivotvorenje medicinske dokumentacije radi postizanja određene imovinske koristi ili krivotvorenje osobnih iskaznica i drugih osobnih dokumenata kojima se služimo u pravnom prometu.

Dostupnost u digitalnom obliku dokumentacije u kojoj su sadržani osobni podaci građana, podaci o poslovnim subjektima te dokumentacija poslovnih subjekata podložni su zlouporabi u vidu krivotvorenja. Krađa podataka koji se vode u digitalnom obliku i krivotvorenje dokumentacije te javnih isprava jedan je od najvećih problema s kojima se svakodnevno suočavamo. Stoga zaštita osjetljivih dokumenata zauzima značajno mjesto u svijetu informatike. Zakon o zaštiti osobnih podataka uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj. Sama svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Isprava je svaki predmet koji je podoban ili određen da služi kao dokaz činjenice koja ima vrijednost za pravne odnose. Polazeći od izdatnika, isprave dijelimo na javne i privatne isprave. Kazneni zakon ne daje definiciju ni javne ni privatne isprave, tako da definiciju pojma javna i privatna isprava nalazimo primjerice u Zakonu o parničnom postupku i Zakonu o općem upravnom postupku. Privatna isprava je izjava volje pojedinca u pisanom obliku, dok je javna isprava posebni oblik isprave koja osim općih pretpostavki koje su neophodne za svaku ispravu u užem smislu, da je u propisanom obliku, mora sadržavati i dodatne uvjete, da ju je u granicama svojih ovlaštenja izdalo državno tijelo ili neko drugo tijelo s javnim ovlastima. Lažna isprava je ona isprava koja ne potječe od osobe koja je na njoj naznačena kao izdavatelj isprave, bilo da se izjava pripisuje osobi koja ju nije dala ili osobi koja uopće ne postoji. Preinačena je ona prava isprava na kojoj je neovlašteno, bitno izmijenjen sadržaj. Isprava koju je u propisanom obliku izdalo državno tijelo u granicama svoje nadležnosti te isprava koju je u takvom obliku izdala pravna ili fizička osoba u obavljanju javnog ovlaštenja koje joj je povjereno zakonom ili propisom utemeljenim na zakonu (javna isprava), dokazuje istinitost onoga što se u njoj potvrđuje ili određuje. [6]

Kao pojam, isprava se pojavljuje kod kaznenih djela protiv vjerodostojnosti isprava i to: krivotvorenje isprave (čl. 278. Kaznenog zakona), krivotvorenje službene ili poslovne isprave (čl. 279. Kaznenog zakona), zlouporaba osobne isprave (čl.280. Kaznenog zakona), ovjeravanje neistinitog sadržaja (čl. 281. Kaznenog zakona), izdavanje i uporaba neistinite liječničke ili veterinarske svjedodžbe (čl. 282. Kaznenog zakona), izradba, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za krivotvorenje isprava (čl. 283. Kaznenog zakona).

Kaznenim zakonom Republike Hrvatske[7] u čl.275.

6 Ana Garačić,sutkinja Vrhovnog suda Republike Hrvatske "Novi kazneni zakon", Organizator, 2013.

7 "Narodne novine" broj 125/2011 i 144/12

st.1. propisano je tko izradi lažni vrijednosni papir koji se izdaje na temelju propisa, preinači pravi vrijednosni papir ili pribavi takav lažni vrijednosni papir ili ga stavi u optjecaj kao pravi kaznit će se kaznom zatvora od jedne do deset godina dok je st. 2. čl. 275. Kaznenog zakona propisano tko lažni vrijednosni papir koji je primio u uvjerenju da je pravi, saznavši da je lažan, stavi u optjecaj, kaznit će se kaznom zatvora do tri godine. Stavkom 3. čl. 275. Kaznenog zakona propisano je da će se lažni vrijednosni papir oduzeti. Kaznenim zakonom propisano je kao kazneno djelo i krivotvorenje isprave pa tako čl. 278. st. 1. Kaznenog zakona propisano je tko izradi lažnu ispravu ili preinači pravu s ciljem da se takva isprava uporabi kao prava ili tko takvu ispravu nabavi radi uporabe ili je uporabi kao pravu, kaznit će se kaznom zatvora do tri godine a kazna je propisana i za onoga tko obmane drugoga o sadržaju kakve isprave i ovaj stavi svoj potpis na tu ispravu, držeći da se potpisuje pod kakvu drugu ispravu ili pod kakav drugi sadržaj kao i za onoga tko kazneno djelo počini glede javne isprave, oporuke, mjenice, čeka, platne kartice ili javne ili službene knjige koja se mora voditi na temelju zakona, Zakonodavac propisuje kao kazneno djelo i krivotvorenje službene ili poslovne isprave[8], ovjeravanje neistinitog sadržaja[9] kao i izdavanje i uporabu neistinite liječničke ili veterinarske edodžbe.[10] Zaštita službenih i/ili poslovnih isprava, osobnih isprava koje izdaju tijela državne i javne uprave spriječila bi zlouporabu takvih isprava, ali bi imala i za cilj sprječavanje nastanka materijalne štete koja je često vezana uz korištenje lažnih isprava u pravnom prometu. Ubrzani napredak informacijskih tehnologija zasigurno može povećati zaštitu javnih poslovnih i osobnih dokumenata unutar kojega procesa treba razmotriti i izradu i izdavanje službenih isprava kao i dokumentacije s posebnim zaštitama koja vrsta zaštite bi povećala sigurnost u pravnom prometu građana kao i poslovnih subjekata.

8 Članak 279. st.1. KZ-a propisano je da službena ili odgovorna osoba koja u službenu ili poslovnu ispravu, knjigu ili spis unese neistinite podatke, ili ne unese kakav važan podatak, ili svojim potpisom, odnosno službenim pečatom ovjeri takvu ispravu, knjigu ili spis s neistinitim sadržajem ili koja svojim potpisom, odnosno službenim pečatom omogući izradbu isprave, knjige ili spisa s neistinitim sadržajem, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

9 Članak 281. st.1. KZ-a propisano je tko dovođenjem u zabludu nadležnog tijela učini da ovo u javnoj ispravi, zapisniku ili knjizi ovjeri štogod neistinito što ima služiti kao dokaz u pravnom prometu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

10 Članak 281. st.1. KZ-a propisano je tko dovođenjem u zabludu nadležnog tijela učini da ovo u javnoj ispravi, zapisniku ili knjizi ovjeri štogod neistinito što ima služiti kao dokaz u pravnom prometu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

3. Novim tehnologijama do smanjenja zloupotreba

3. *New technologies to reduce misuse*

Razvoj grafičkih i usporedno informatičkih rješenja u zaštiti ispisa dokumenata daju nam sasvim nove mogućnosti. Kombiniranjem aktivnih zaštita sa pasivnim te povezivanjem na pripadajuće online baze pokušat će se potpuno minimizirati kriminalne aktivnosti. Višestrukom zaštitom dokumenata smanjuje se mogućnost zlouporabe, odnosno mogućnosti krivotvorenja ispisanih dokumenata. Sustav[11] koji bi se pokazao kao kvalitetno rješenje je sustav za višestruku zaštitu ispisa dokumenata koji pruža mogućnost višestruke zaštite ispisa dokumenata i njihovo sigurno arhiviranje. Stoga bi glavni zahtjevi na takav sustav bili:

1. Sustav treba bazirati na tzv. on-site (na licu mjesta) i online (u trenutku ispisa) zaštitu ispisa dokumenata.
2. Sustav je kombinacija hardverskog i softverskog rješenja.
3. Sustav treba biti skalabilan i prilagodljiv korisničkoj infrastrukturi
4. Zaštita je višestruka - grafička i kriptiranje tajnim ključem, sa ili bez barkoda.
5. Sve zaštite koje se mogu ugraditi u sustav ovise isključivo o izboru pisača koje korisnik ima.
6. Sustav ne smije koristiti nikakav poseban hardver ili softver
7. Klijent – korisnik sustava ne smije imati nikakve dodatne radnji pri zaštiti ispisa dokumenata
8. Sustav treba ponuditi i e-verziju štićenog dokumenta sa mogućnosti slanja na adresu

11 Ivan Rajković, Jana Žiljak Vujić, Ognjen Mitrović, Slaven Crnjac, Razvoj rješenja sigurnog ispisa u privatnim mrežama, Međunarodni znanstveni skup TISKARSTVO & DIZAJN 2015., Zagreb, Hrvatska

e-pošte ili pohrane na uređaj za pohranu podataka

9. Sustav treba biti kompatibilan sa DMS[12] sustavom
10. Sva komunikacija između korisnika sustava, poslužitelja za ispis dokumenata te pisača mora biti sigurna.

Za razliku od nesigurne veze u tradicionalnim sustavima, u rješenju koje se ovdje opisuje uspostavljena je sigurna veza cijelim komunikacijskim putem od klijenta do pisača (prikazano na slici 1). Cijeli postupak se u kratko može podijeliti u tri koraka:

Korak 1. uspostavlja se sigurno komunikacija između poslužitelja za višestruki sigurni ispis i kompatibilnog pisača. Za ovu komunikaciju se koriste izolirane VLAN mreže odvojene logički ili fizički od ostatke lokalne mreže putem preklopnika i/ili usmjernika/vatrozida. Kao kvalitetno i ekonomski isplativo rješenje može se izabrati Mikrotik vatrozid / usmjernik. Njegove performanse ne zaostaju puno za vodećim proizvođačima hardvera a cijenom su za red veličine jeftiniji.

Korak 2. lokalno računalo korisnika se spaja kroz sigurni komunikacijski kanal na poslužitelj za višestruku zaštitu ispisa.

Korak 3. Nakon uspostave veze u koraku 1 između poslužitelja i pisača te u koraku 2 između klijentskog računala i poslužitelja, korisnik može poslati na ispis dokument koji se ispisuje sa svim zaštitama na pisaču.

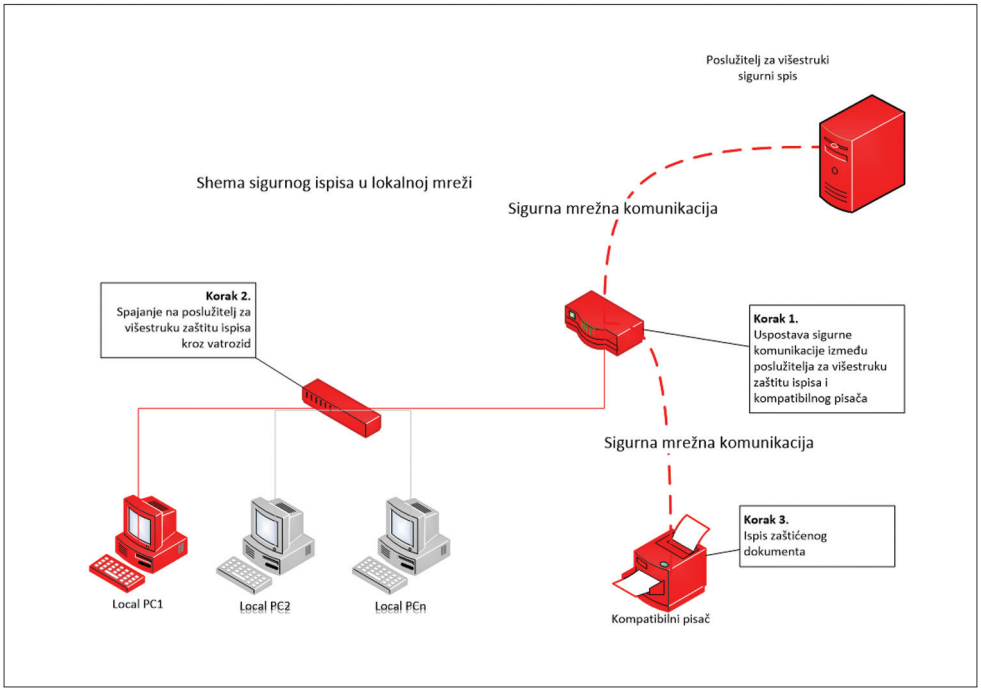
U idejnom rješenju korišteni su uređaji Mikrotik usmjernici i Cisco ili Mikrotik preklopnici. Crveno obojeni uređaji na slici 1 prikazuju aktivnu liniju uređaja u trenutku ispisa, a crvena linija prikazuje aktivni sigurni komunikacijski put.

Kako je već prije navedeno, ovo rješenje treba biti skalabilno te imati mogućnost implementacija u različitim uvjetima gdje korisnik ima više ureda ili više različitih fizičkih lokacija. Na slici 2. prikazano je kada korisnik ima više ureda i jedan kompatibilni pisač na kojem vrši sigurni ispis zaštićenih dokumenata[13].

Na slici 3. prikazano je cjelokupno rješenje sa koracima u procesu zaštite ispisa dokumenta.

Prvi korak je gdje korisnik sa svog računala šalje nezaštićeni dokument na ispis. U ovom koraku je potrebno osigurati da korisnik na svom računalu ima:

- Ispravno podešene upravljačke programe za ispis na kompatibilni pisač
- Ima ostvarenu komunikaciju prema poslužitelju za višestruku zaštitu ispisa dokumenata

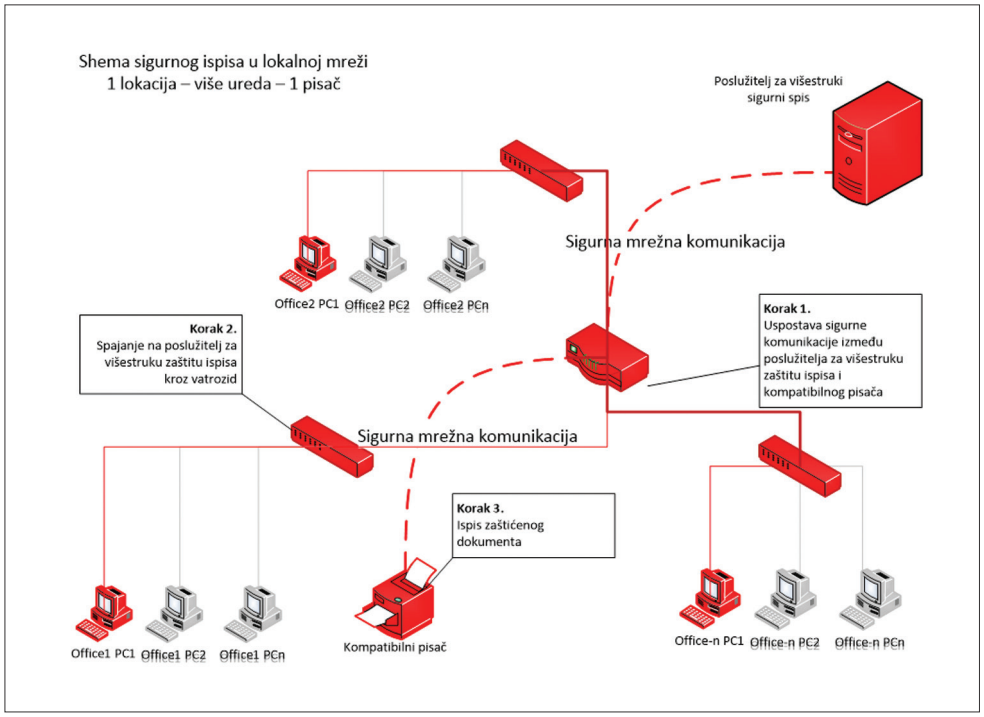


Slika 1
Shema sigurnog ispisa u lokalnoj mreži

Figure 1
Showing secure printing schemes at multiple offices with one printer

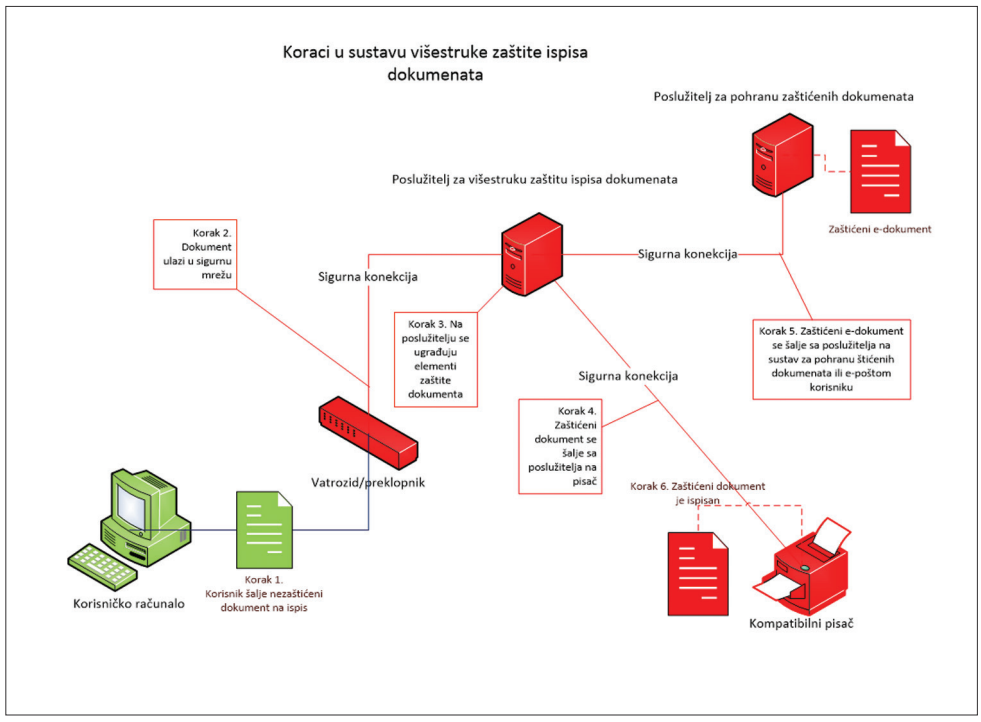
12 DMS – Document management System – Sustav za upravljanje dokumentima

13 Jana Žiljak Vujić, Slaven Crnjac, Ognjen Mitrović, The Development of Secure Printing Solutions in Private Networks, INTERNATIONAL DESIGN CONFERENCE - DESIGN 2016



Slika 2
Prikaz sheme sigurnog ispisa kod više ureda sa jednim pisačem

Figure 2
Showing secure printing schemes at multiple offices with one printer



Slika 3
Prikaz koraka u postupku zaštite ispisa dokumenta

Figure 3
Showing steps in procedure of document Printing protection

U drugom koraku dokument ulazi u zaštićeni komunikacijski put nakon što prođe usmjernik i/ili vatrozid. U ovom rješenju se koristio Mikrotik usmjernik. U ovom trenutku dokument više nitko ne može preuzeti niti mu na bilo koji način neovlašteno pristupiti.

Treći, četvrti, peti i šesti koraci su ključni u ovom rješenju. U ovom dijelu dokument dolazi na poslužitelj za višestruku zaštitu ispisa dokumenata. Ovdje je bitno naglasiti da je bio pravilan odabir Debian operativnog sustava i CUPS[14] poslužitelja. Nizom besplatnih alata koji su dostupni na Debian operativnom sustavu omogućava se provedba zaštite u više faza. Na slici 4 prikazane su faze zaštite dokumenta na poslužitelju. Ukupno je pet faza kroz koje prolazi svaki dokument.

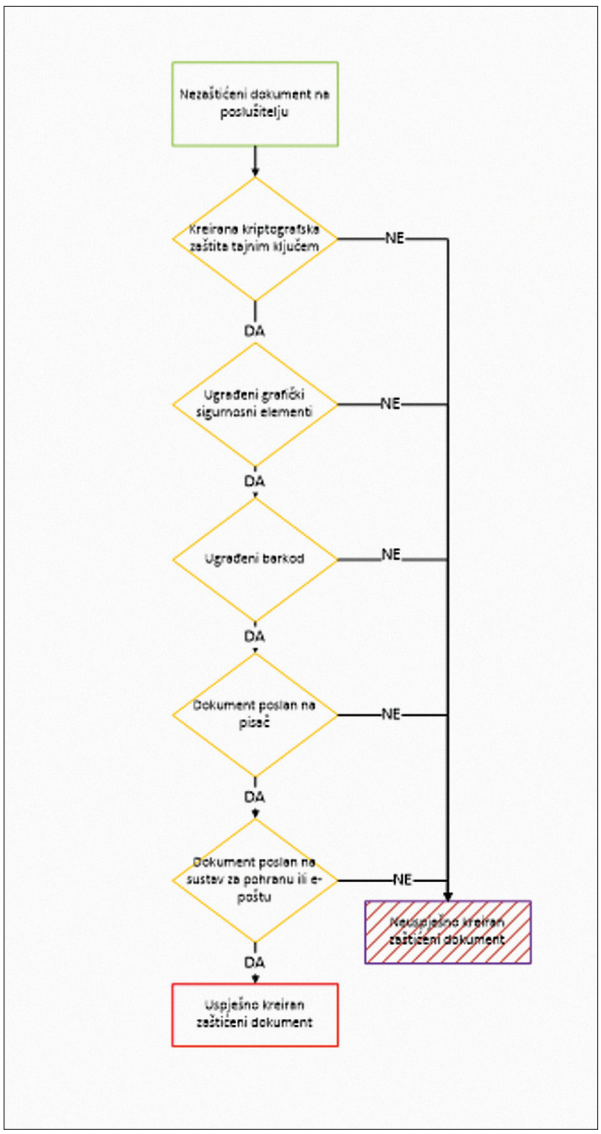
- Prva faza je faza kreiranja digitalnih kriptografskih ključeva
- Druga faza je ugradnja grafičkih sigurnosnih

14 CUPS Common Unix Printing System

elemenata iz unaprijed pripremljenog predloška.

- Treća faza je kreiranje barkoda
- Četvrta faza je slanje dokumenta na pisač

Peta faza slanje e-dokumenta na sustav za pohranu dokumenata ili na adresu e-pošte. Ukoliko je dokument uspješno prošao kroz sve faze, može se govoriti o uspješno završenom postupku zaštite dokumenta. Bilo koja faza da nije napravljena, dokument nije zaštićen.



Slika 4 *Faze kreiranja zaštite na poslužitelju*

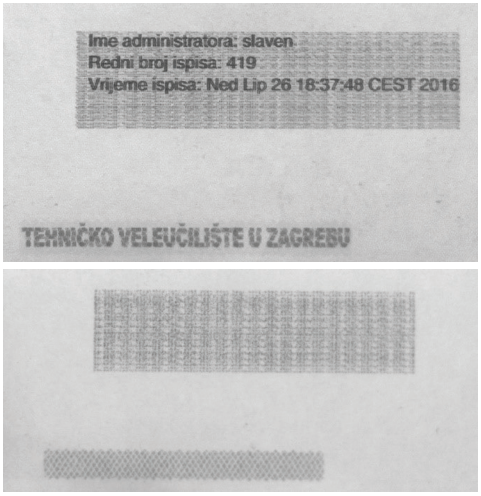
Figure 4 *Phases of creating protection on the server*

3.1 Testiranje rješenja

3.1 *Testing solutions*

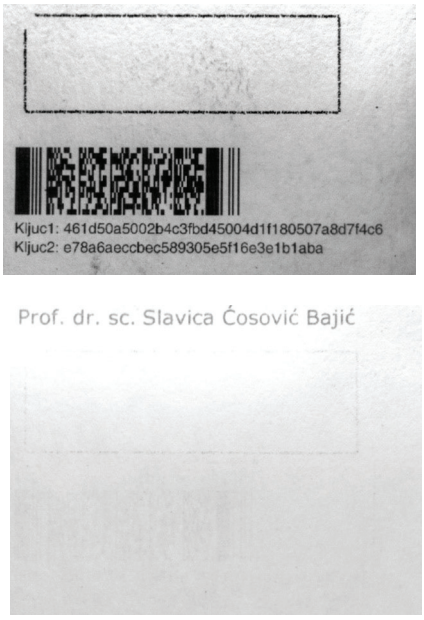
Rješenje je testirano na Tehničkom veleučilištu u Zagrebu (u daljnjem tekstu TVZ).

Slika 6(lijevo izvornik – desno kopija) pokazuje u IR području elemente zaštite koji inače nisu vidljivi u vidljivom spektru. S vrha prema dolje nalaze se tri linije teksta koje se dinamički mijenjaju i dodaju na poslužitelju te ovise o osobi koja ispisuje dokument, rednim brojem ispisa te trenutku ispisa. Na dnu same slike je prikazana IR slika iz dualne zaštite infrareddesign[15] tehnologijom.



Slika 6 *Grafički elementi zaštite u IR spektru*

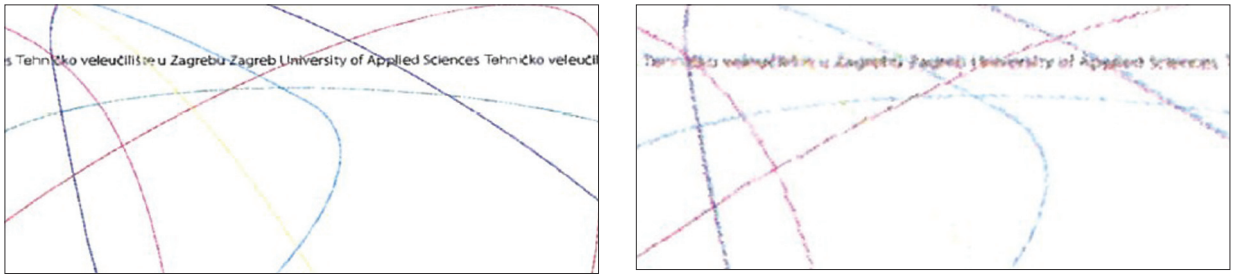
Figure 6 *Graphic elements of protection in the IR spectrum*



Slika 7 *Grafički elementi zaštite u IR spektru 2*

Figure 7 *Graphic elements of protection in the IR spectrum no.2*

15 Ivana Žiljak, Klaudio Pap, Jana Žiljak Vujić, Infrared Security Graphics,2009. Zagreb, knjiga, ISBN 978-953-7064-11-2



Slika 8 *Elementi grafičke zaštite pod uvećanjem*

Figure 8 *Elements of graphic protection under magnification*

Slike 7 prikazuju grafičke elemente zaštite potvrde o studiranju Tehničkog veleučilišta u i IR spektru na izvorniku (lijevo) i kopiji (desno)
Na slici 8 prikazani su uvećano 400% dio elemenata zaštite mikro tekstom i krivuljama. Može se primijetiti da su i pri tom povećanju tekst i krivulje na izvorniku zadržale svoj integritet a na kopiji je integritet narušen.

4. Zaključak

4. *Conclusion*

Sustav rješenja sigurnog ispisa u privatnim mrežama donosi novi način upravljanja ispisom u uredima. Ekonomičnost, sigurnost, skalabilnost, upravljivost su glavne prednosti ovako dizajniranog sustava. Korisnici koji imaju implementiran sustav mogu se osloniti na sigurnu distribuciju dokumenata sa ugrađenom infrared i kriptografskom zaštitom a krajnji korisnici dokumenata imaju mogućnost provjere vjerodostojnosti ispisanog izvornika. Prednost u odnosu na klasični sustav osim infrared zaštite je upravljivost sustavom te smanje potreba za lokalnom administracijom upravljanja ispisom.

AUTOR · AUTHOR

Jana Žiljak Vujić- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 1, No. 1, 2013.

Ljiljana Matuško Antonić
Pravni fakultet u Zagrebu upisala sam akademske godine 1982/83, a diplomirala sam 1986. godine. Nakon završenog Pravnog fakulteta radila sam kao odvjetnički vježbenik te sam 1988. godine položila pravosudni ispit. Dana 28. prosinca 2011. godine stekla sam znanstveni stupanj doktorice znanosti iz područja građanskih znanosti (tema disertacije: Uspostava pravnog jedinstva nekretnina na građevinskom zemljištu u postupku preoblikovanja zemljišnih knjiga). Na Tehničkom veleučilištu u Zagrebu imenovana sam uz suglasnost Pravnog fakulteta u Zagrebu za predavača na predmetu "Poslovna etika i pravo" od šk.g. 2009/2010. Autor sam više stručnih članaka. Pregledni znanstveni rad objavila sam 2014. godine pod nazivom „Kriteriji za naknadu neimovinske štete fizičkih osoba“, Liber amicorum in honorem Vilim Gorenc, Pravni fakultet Sveučilišta u Rijeci, Zavod za građansko pravo, 2014.

Slaven Crnjac- nepromjenjena biografija nalazi se u časopisu Polytechnic & Design Vol. 4, No. 1, 2016.