PREGLEDNI ZNANSTVENI ČLANAK

UDK: 088.22(497.13)
343.982:004.932.72'1
57.087.1:004
Primljeno: ožujak 2012.

JASMINKA PEROŠ*, GORDAN MRŠIĆ**, NEVENKA ŠKAVIĆ***

Uvođenje biometrije u putne isprave[1]

Sažetak

Susrećući se s rastućim problemom krivotvorenih putnih isprava i zloporabom originalnih isprava koje olakšavaju kretanje terorističkih i ostalih kriminalnih skupina, međunarodne se aktivnosti usmjeravaju na usklađivanje načina zaštite putnih isprava, uspostavljanje učinkovitog nadzora nad njihovim izdavanjem te kontrole putnika i putnih isprava na graničnim prijelazima. U cilju sprječavanja takvih kretanja i pridonošenja sveopćoj sigurnosti, na međunarodnoj su razini utvrđene specifikacije i preporuke vezane uz uvođenje biometrijskih elektroničkih putovnica – strojno čitljivih putovnica koje uz, već tradicionalne vizualne i optički čitljive karakteristike, sadrže i biometrijske značajke nositelja isprave koje se u digitalnom obliku pohranjuju na beskontaktni čip u putovnici. Prednosti uvođenja biometrijskih e-putovnica, u pogledu uspostavljanja više razine sigurnosti međunarodnog kretanja osoba kroz dodatnu verifikaciju identiteta nositelja isprave, zasigurno su nedvojbene, no istodobno se nameće pitanje zaštite povjerljivosti biometrijskih značajki pohranjenih na čipu e-putovnica.

U članku je opisana primjena biometrijske tehnologije u zaštiti putnih isprava s posebnim naglaskom na međunarodnu, europsku i nacionalnu zakonsku regulativu uvođenja biometrijskih e-putovnica, mehanizme zaštite digitalnih podataka, te značaj uspostavljanja sustava upravljanja identitetom na području sigurnosti putnih isprava, u širem smislu.

Ključne riječi: *biometrija, biometrijske e-putovnice, mehanizmi zaštite digitalnih podataka, infrastruktura javnog ključa, sustavi upravljanja identitetom.*

---

* Jasminka Peroš, mag. forenzike.

** dr. sc. Gordan Mršić, načelnik Centra za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić".

*** Nevenka Škavić, struč. spec. krim., samostalni vještak za novčanice, dokumente i rukopise Centra za forenzična ispitivanja, istraživanja i vještačenja "Ivan Vučetić".

[1] Za potrebe ovog rada, autori su se vodili definicijom Međunarodne organizacije civilnog zrakoplovstva prema kojoj je putna isprava (eng. *travel document*) javna isprava izdana od strane države ili organizacije koja služi za međunarodna putovanja (npr. putovnica, viza i isprava kojom se dokazuje identitet).

UVOD

Pojam biometrija dolazi od grčke riječi *bios* (život) i *metrics* (mjera) te označava mjerljive fizičke i ponašajne karakteristike[2] živih bića, odnosno osoba. Sukladno s time, biometrijsku je tehnologiju moguće definirati kao automatiziranu metodu identifikacije ili verifikacije osoba utemeljenu na njihovim fizičkim i ponašajnim karakteristikama (Bača, 2004:342).

Iako je povijest biometrije stara gotovo koliko i čovječanstvo, pri čemu su ideje mnogih suvremenih automatiziranih biometrijskih sustava začete već stotinama, čak i tisućama godina prije, početci biometrijske tehnologije usko se vezuju uz razvitak informacijske tehnologije, čiji je neslućeni procvat posljednjih desetljeća otvorio mnogobrojne mogućnosti njezine primjene u raznovrsnim područjima ljudskoga društva. Premda biometrijska tehnologija mjeri različite biometrijske karakteristike na različite načine ovisno o području primjene, svi biometrijski sustavi obuhvaćaju iste procese koji su podijeljeni u dvije razine. Prvu razinu čini registracija biometrijskih karakteristika[3] (eng. *enrollment*), dok druga razina uključuje postupak identifikacije[4] (eng. *identification*) ili verifikacije[5] (eng. *Verification*), (Nimac, 2007).

Sigurnost suvremenog društva sve više ovisi o mogućnostima pouzdane identifikacije ili verifikacije osoba, pri čemu je biometrijska tehnologija postala neizostavan dio svakodnevice. Javni sektor koristi biometrijsku tehnologiju više od desetljeća, usmjeravajući se na fizičke karakteristike poput otisaka prstiju, biometrije lica, šarenice oka, geometrije dlana ili retine oka, dok se ponašajne karakteristike, poput dinamike potpisa ili glasa, sve češće uvode u svrhu kontrole pristupa ili registracije birača (Silicon Trust, 2008). Jednako tako, tijela državne vlasti žele biti nedvojbeno sigurna u identitet osoba s kojima dolaze u doticaj, pa stoga usmjeravaju vlastite napore k uvođenju biometrijske tehnologije u razne segmente državne uprave, a što se očituje u značajnom pomaku koji je posljednjih godina učinjen na području zaštićenih isprava po pitanju standardizacije, međunarodne interoperativnosti[6], te privatnosti i sigurnosti (Grijpink, 2010).

---

[2] U skupinu fizičkih biometrijskih karakteristika potpadaju otisci prstiju, geometrija dlana, geometrija lica, šarenica i mrežnica oka, DNK i slično, dok su neke od ponašajnih biometrijskih karakteristika boja glasa, dinamika tipkanja, dinamika vlastoručnog potpisa i hod.

[3] Prilikom postupka registracije, osoba prezentira vlastite biometrijske karakteristike, poput otiska prsta ili šarenice oka, na za to predviđenim uređajima. Značajna obilježja osobe se lociraju, jedan ili više primjera se izoliraju, kodiraju i pohranjuju kao referentni obrazac (eng. *template*) u bazu podataka biometrijskog sustava i/ili identifikacijsku ispravu u svrhu buduće usporedbe.

[4] Pojam identifikacije odnosi se na postupak utvrđivanja identiteta osobe. Sustav za identifikaciju provodi usporedbu u omjeru 1 : N, uspoređujući probni obrazac sa svim referentnim obrascima pohranjenima u bazi podataka sustava, s ciljem pronalaska podudarnosti probnog obrasca s nekim od referentnih obrazaca, odnosno dobivanja odgovara na pitanje "tko je ta osoba".

[5] Verifikacija je postupak provjere ili potvrđivanja identiteta osobe, odnosno postupak kojim se dokazuje je li osoba zaista ona za koju se predstavlja. Sustav za verifikaciju provodi usporedbu u omjeru 1 : 1, uspoređujući probni obrazac s referentnim obrascem pohranjenim u bazi podataka sustava ili u identifikacijskom dokumentu, a s ciljem utvrđivanja njihove međusobne podudarnosti.

[6] Međunarodna interoperativnost je sposobnost inspekcijskog sustava da razmjenjuje podatke s drugim državama diljem svijeta, obrađuje podatke dobivene od sustava drugih država i koristi ih u vlastitim inspekcijskim postupcima. Osnovu inspekcijskog sustava čine inspekcijski uređaji, tj. posebni čitači koji omogućavaju optičko čitanje strojno čitljive zone i čitanje digitalnih podataka pohranjenih na čipu e-isprava.

1. PRIMJENA BIOMETRIJE U PUTNIM ISPRAVAMA

Zbog svoga su značaja, putne isprave oduvijek bile u središtu zanimanja krivotvoritelja i drugih kriminalnih skupina – bilo u obliku potpunog i djelomičnog krivotvorenja, bilo u obliku zloporabe tuđe isprave (eng. *look-alike fraud*), (Broekhaar, 2011). Kako bi se umanjila mogućnost njihova krivotvorenja i zloporabe, Međunarodna organizacija civilnog zrakoplovstva (eng. *International Civil Aviation Organization*, u daljnjem tekstu: ICAO)[7] tijekom godina je izradila specifikacije vezane uz izgled, sadržaj, zaštitne elemente te druge sadržaje izrade i izdavanja putnih isprava. Standardizacijom putnih isprava, s jedne se strane olakšalo međunarodno kretanje osoba, dok se s druge strane ojačala sveobuhvatna sigurnost kroz mogućnost vizualne provjere vjerodostojnosti putnih isprava (Broekhaar, 2011). Daljnji korak u razvijanju standarda vezanih uz izdavanje putnih dokumenata bio je uvođenje strojno čitljive zone[8] (eng. *machine readable zone* – MRZ), što je omogućilo automatiziranu provjeru vjerodostojnosti isprava uporabom optičkog čitača. Putne isprave koje, osim vizualnih, sadrže i strojno čitljive podatke ispisane sukladno s ovim specifikacijama nazivaju se **strojno čitljivim putnim ispravama** (eng. *machine readable travel documents*).

Izuzetno bitan aspekt međunarodne sigurnosti predstavlja i mogućnost verifikacije nositelja putne isprave, odnosno potvrđivanje je li osoba koja predočava putnu ispravu na graničnom prijelazu uistinu ona kojoj je tâ putna isprava prvotno i izdana. U cilju poboljšanja sigurnosnih značajki putnih isprava, kroz snažnije povezivanje isprave s njezinim nositeljem, ICAO je izradio globalne smjernice vezane uz implementaciju biometrije u putovnice i druge putne isprave. Uvođenjem biometrije u putovnice omogućena je automatizirana usporedba biometrijskih značajki pohranjenih na čipu e-putovnice s nositeljem putovnice tijekom granične kontrole. Putovnica koja, sukladno s ICAO specifikacijama, posjeduje ugrađen beskontaktni čip s biometrijskim podacima naziva se **e-putovnica**.

Osim globalnog trenda uvođenja biometrijskih e-putovnica, pojedine su države učinile dodatan korak na području zaštite isprava, uvođenjem biometrijskih e-osobnih iskaznica i implementiranjem viznih sustava koji se oslanjaju na biometrijsku tehnologiju.

Primjerice, potkraj 2010. godine Savezna Republika Njemačka je započela s izdavanjem nacionalnih e-osobnih iskaznica koje posjeduju beskontaktni čip ugrađen u strukturu polikarbonatne kartice, čime su omogućene *online* funkcije poput e-poslovanja, e-uprave i internetskog bankarstva, kao i mogućnost digitalnog potpisivanja. Pritom je građanima ostavljena sloboda u određivanju opsega u kojem će koristiti ponuđene im *online* aplikacije. Istodobno, stavljen je naglasak na zaštitu podataka i mjere osiguravanja privatnosti. Obvezatni digitalni podaci sadržani na čipu uključuju strojno čitljivu zonu i digitalnu fotografiju vlasnika dokumenta, dok je svakom građaninu ostavljeno na odluku želi li

[7] ICAO je organizacija Ujedinjenih naroda nadležna za uspostavljanje međunarodnih specifikacija i preporuka vezanih uz izdavanje putovnica i ostalih putnih isprava.

[8] Strojno čitljivu zonu čine dvije linije podataka na individualizacijskoj stranici putne isprave koje sadrže standardiziran prikaz tipa isprave, kôda države izdavateljice, imena i prezimena nositelja, serijskog broja putne isprave, datuma rođenja nositelja, datuma valjanosti putne isprave, kao i pripadajućih, aritmetički izvedenih kontrolnih brojeva.

na čip pohraniti i dodatne biometrijske karakteristike u vidu otisaka prstiju. Uvođenje e-osobne iskaznice od strane Savezne Republike Njemačke odličan je primjer kako udovoljiti suvremenim potrebama svojih građana (Broekhaar, 2011). Potrebno je naglasiti kako je stvarni potencijal implementacije e-osobne iskaznice moguće dosegnuti jedino ukoliko građani imaju povjerenja u državu izdavateljicu, odnosno ukoliko vjeruju u sigurnosne značajke takve e-isprave i spremni su je rabiti u svakodnevnom životu. Upravo iz toga razloga, sigurnosni aspekti u obliku učinkovitih mehanizama zaštite digitalnih podataka pohranjenih na čipu imaju ključnu ulogu (Reisen, 2008).

Rasprava vezana uz elektroničke vize započela je još u studenome 1999. godine, dok je 2004. godine predloženo da se u postojeću naljepnicu vize ugradi beskontaktni čip. ICAO je preuzeo odgovornost za razvijanje navedenih specifikacija, no nakon višegodišnjeg intenzivnog istraživanja te uzimanja u obzir svih tehničkih i operativnih aspekata održivosti navedenoga pristupa, 2009. godine na svjetskoj je razini postignut konsenzus kojim se odustalo od ideje uvođenja beskontaktnog čipa u naljepnicu vize. Umjesto toga odlučeno je usmjeriti napore k uspostavljanju viznih sustava s bazom podataka biometrijskih karakteristika, pri čemu se ICAO obvezao razviti smjernice vezane uz aplikativnu shemu sustava izdavanja viza. Sjedinjene Američke Države još su 2004. godine uspostavile US-VISIT program vezan uz zaprimanje zahtjeva za izdavanje viza u američkim ambasadama diljem svijeta, provjeru identiteta nositelja vize prilikom ulaska u SAD i napuštanja teritorija države, a koji obuhvaća skup koordiniranih sigurnosnih mjera koje se oslanjaju na biometrijsku tehnologiju (Reisen, 2008). Na razini Europske unije utvrđen je jedinstven format viza zemalja članica[9] i uspostavljen središnji Vizni informacijski sustav (eng. *Visa Information System* – VIS)[10] čiji je sastavni dio baza podataka biometrijskih značajki, i to digitalne fotografije i otisaka svih deset prstiju podnositelja zahtjeva za izdavanje vize, sukladno s ICAO specifikacijama. Po uzoru na europsku praksu, u studenom 2011. godine Republika Hrvatska donijela je novi Zakon o strancima[11] prema kojem se svi zahtjevi za izdavanje vize pohranjuju i obrađuju u Hrvatskom viznom informacijskom sustavu (tzv. Hrvatski VIS), kao i podaci o izdanim, produljenim, odbijenim, poništenim i ukinutim vizama. Zakonom je propisano prikupljanje biometrijskih podataka – digitalne fotografije i otisaka deset prstiju, sukladno s ICAO i specifikacijama Europske unije, čime je postavljen temelj za povezivanje s VIS-om ulaskom u Europsku uniju.

Uvođenje biometrije u putne isprave omogućava automatiziranu provjeru identiteta nositelja isprave, pridonosi sigurnosti proizvodnje, izdavanja i postupka utvrđivanja vjerodostojnosti zaštićenih dokumenata, te osigurava bolje povezivanje identiteta osobe – nositelja dokumenta, sa samim dokumentom. Međutim, pritom se nikako ne smije zanemariti činjenica da su biometrijske e-isprave još uvijek i tradicionalno zaštićene isprave koje su zadržale sve dotadašnje elemente zaštite, poput vodenog znaka, optički promjenjive tinte, UV-zaštitnih elemenata i slično, odnosno elemente zaštite koji i dalje podliježu provjerama radi utvrđivanja njihove vjerodostojnosti (Ellis, 2009).

---

[9] Uredba Vijeća Europe (EC) 1683/95. i 334/2002. o jedinstvenom formatu viza zemalja članica.
[10] Uredba Vijeća 2004/512/EC o osnivanju Viznog informacijskog sustava (VIS) i Uredba Vijeća 2006/648/EC vezana uz tehničke specifikacije o standardima za pohranu biometrijskih značajki u VIS.
[11] Zakon o strancima. (NN 130/11.)

2. PRAVNI OKVIR UVOĐENJA BIOMETRIJSKIH E-PUTOVNICA

2.1. ICAO – globalne smjernice vezane uz biometrijske e-putovnice

Kako je već ranije spomenuto, ICAO je 2004. godine izradio globalne smjernice vezane uz biometrijske e-putovnice u kojima ističe kako je prilikom uvođenja biometrije u putovnice i druge putne dokumente neophodno voditi brigu o globalnoj interoperativnosti, jednoobraznosti, tehničkoj pouzdanosti, praktičnosti i trajnosti (Broekhaar, 2011).

Nakon detaljnog razmatranja dostupnih biometrijskih tehnologija, ICAO je usvojio biometriju lica kao primarnu i obveznu biometrijsku značajku, dok su kao sekundarne, proizvoljne biometrijske značajke koje države izdavateljice mogu pohraniti na čip e-putovnica, usvojene – biometrija otiska prsta i šarenice oka. Nekoliko je razloga zbog kojih je biometrija lica odabrana kao primarna i obvezatna biometrijska značajka koja će se koristiti u identifikacijske i verifikacijske svrhe, a neki od kojih su sljedeći:

- biometrija lica ne otkriva dodatne informacije, osim onih koje osoba ionako pokazuje u javnosti, te je društveno i kulturalno prihvaćena diljem svijeta
- biometrija lica već se dugi niz godina rutinski prikuplja i provjerava prilikom kontrole isprava
- javnost je upoznata s postupkom prikupljanja uzoraka i njihova korištenja u identifikacijske ili verifikacijske svrhe
- uvođenje biometrije lica ne zahtijeva novu, skupocjenu tehnologiju
- mnoge države već posjeduju baze podataka ili registre u kojima su pohranjene biometrijske karakteristike lica (fotografije) svojih državljana
- verifikacija fizičke osobe nasuprot digitalne fotografije relativno je jednostavan i uhodan postupak prilikom granične kontrole putnika (Broekhaar, 2011).

Nadalje, kao medij za pohranu biometrijskih podataka nositelja isprave u e-putovnicama odabran je beskontaktni RFID čip s antenom[12] koji treba biti odgovarajućeg kapaciteta (minimalno 32 kB) i omogućavati velike brzine čitanja digitalnih podataka s udaljenosti unutar 10 centimetara.

Radi osiguranja međunarodne interoperativnosti automatizirane provjere digitalnih podataka pohranjenih na čipu, ICAO je uveo jedinstven način organiziranja i pohrane podataka na čipu, tzv. logičku strukturu podataka (eng. *Logical Data Structure*) kojim su utvrđeni svi obvezni i opcionalni elementi podataka (eng. *data elements*) te njihov redoslijed i/ili grupiranje kojih se moraju pridržavati države izdavateljice radi postizanja međunarodne interoperativnosti strojnog čitanja e-putovnica. Logička struktura podataka hijerarhijski je organiziran datotečni sustav, gdje se srodni elementi podataka grupiraju u tzv. skupine podataka (eng. *Data Groups* – DG), koje su brojčano označene od 1 do 16 te pohranjene u osnovne datoteke (eng. *Elementary Files* – EFs). Prema ICAO specifikacijama, skupine podataka 1 i 2 predstavljaju obvezne digitalne podatke koji se pohranjuju na čip e-putovnica, dok su ostale opcionalne (ICAO, 2008).

[12] Beskontaktni RFID čip mora biti sukladan sa standardom ISO/IEC 14443 i treba posjedovati operacijski sustav prilagođen standardu ISO/IEC 7816-4 i 7816-6.

DG1	digitalan zapis strojno čitljive zone
DG2	digitalan zapis fotografije lica nositelja e-putovnice
DG3	digitalan zapis otiska prsta(iju)
DG4	digitalan zapis šarenice(a) oka
DG5-7	identifikacijske značajke nositelja putovnice prikazane na individualizacijskoj stranici (npr. potpis nositelja)
DG8-10	sigurnosne značajke
DG11-13	dodatni i opcionalni podaci
DG14	javni ključ za autentifikaciju čipa
DG15	javni ključ za aktivnu autentifikaciju
DG16	kontakt osoba(e)

Tablica 1: Skupine podataka unutar logičke strukture podataka

Pritom, svaki element podataka posjeduje ***jedinstvenu identifikacijsku oznaku (tag)*** koja državi primateljici omogućava utvrđivanje prisutnosti pojedine skupine podataka u bloku podataka zapisanih od strane države izdavateljice. Lista tagova, odnosno postojećih skupina podataka, pohranjena je u zasebnoj osnovnoj datoteci, tzv. EF.COM. Osim toga, na čipu se nalazi i osnovna datoteka EF.SOD u koju se pohranjuje sigurnosni objekt dokumenta (eng. *Security Object for the Document* – SO_D). Sigurnosni objekt dokumenta sadrži listu *hash* vrijednosti svake pojedine skupine podataka koji su, kao i sam SO_D, digitalno potpisani od strane države izdavateljice radi zaštite logične strukture podataka i omogućavanja državi primateljici provjeru autentičnosti i integriteta digitalnih podataka pohranjenih na čipu. Ukoliko čip podržava mehanizam proširene kontrole pristupa, u datoteci EF.CVCA se pohranjuje CVCA certifikat države izdavateljice e-putovnice. Pristup drugim datotekama na čipu nije dopušten jer sadrže tajne ključeve, poput tajnog ključa za aktivnu autentifikaciju ili ključeva za osnovni pristup dokumentu. Kako završni korak individualizacije e-putovnice uključuje zaključavanje čipa, digitalni podaci pohranjeni na čipu namijenjeni su isključivo za čitanje.

Zaštita obrasca i vizualnog sadržaja putovnica implementiranjem različitih zaštitnih elemenata uvriježen je način zaštite od krivotvorenja koji državama primateljicama ujedno omogućava provjeru vjerodostojnosti putnih isprava. Međutim, uvođenjem biometrijskih e-putovnica javila se potreba za dodatnom zaštitom povjerljivosti, autentičnosti i integriteta digitalnih podataka na čipu e-putovnica. U svrhu zaštite digitalnih podataka pohranjenih na čipu, ICAO je propisao obvezatne i opcionalne kriptografske mehanizme zaštite. Pritom je pasivna autentifikacija utvrđena kao obvezan mehanizam zaštite, dok mehanizme aktivne autentifikacije i osnovne kontrole pristupa ICAO navodi kao opcionalne, pa je odluka o njihovom uvođenju isključivo u nadležnosti države izdavateljice e-putovnice.

Budući da su digitalna fotografija lica nositelja i strojno čitljiva zona sadržane i u vizualnom dijelu e-putovnice na individualizacijskoj stranici isprave, isti se ne smatraju osjetljivim podacima, pa ih je dovoljno zaštititi mehanizmom osnovne kontrole pristupa. Međutim, osim biometrije lica, ICAO ostavlja i mogućnost pohrane dodatnih biometrijskih značajki na čip e-putovnica – otisaka prstiju i šarenice oka, koje se smatraju osjetljivim podacima, te im je pristup potrebno dodatno ograničiti. U tu svrhu, ICAO preporuča dva mehanizma zaštite – proširenu kontrolu pristupa i kriptiranje podataka. No kako u svojim

specifikacijama ne navodi standarde vezane uz njihovo uvođenje, implementacija i zaštita dodatnih biometrijskih značajki ostavljena je u nadležnost državama izdavateljicama. Pojedine države, koje su se odlučile za implementiranje dodatnih biometrijskih značajki u nacionalne e-putovnice, poput zemalja članica Europske unije, odabrale su proširenu kontrolu pristupa nad kriptiranjem podataka jer se potonji mehanizam zaštite pokazao ranjivim na napade grubom silom (ICAO, 2008).

2.2. Zakonska regulativa Europske unije

Sukladno s ICAO preporukama, Vijeće Europske unije donijelo je Uredbu br. 2252/2004. i 444/2009. o standardima zaštite i biometriji u putovnicama i putnim dokumentima izdanim od strane zemalja članica, kojom je obvezalo države članice da najkasnije do 28. lipnja 2006. godine započnu s izdavanjem e-putovnica s digitaliziranom fotografijom vlasnika putovnice pohranjenom na beskontaktnom čipu, dok je za integriranje otisaka prstiju na čip, i to kažiprsta lijeve i desne ruke, ostavljen rok do 28. lipnja 2009. godine. Pri uvođenju e-putovnica tzv. *prve generacije* – putovnica koje od biometrijskih karakteristika sadržavaju samo digitaliziranu fotografiju lica, zemlje članice Europske unije utvrdile su pasivnu autentifikaciju i osnovnu kontrolu pristupa kao obvezne mehanizme zaštite, dok je aktivna autentifikacija ostavljena kao opcionalna.

Kod uvođenja e-putovnica tzv. *druge generacije* – putovnica koje na čipu uz digitalnu fotografiju lica sadrže i otiske prstiju, osim ranije spomenutih, obveznih i opcionalnih mehanizama, Europska je unija za zaštitu otisaka prstiju digitalno pohranjenih na čipu razvila i dodatan, obvezatan mehanizam proširene kontrole pristupa (Hornung, 2007).

2.3. Nacionalna regulativa uvođenja e-putovnice hrvatskih državljana

Razina zaštite prve hrvatske putovnice, s čijim se izdavanjem započelo u listopadu 1991. godine[13], bila je prilagođena tadašnjim uvjetima i tehnologijama, kao i mogućoj tehničkoj izradi. Postupak individualizacije bio je decentraliziran, odnosno osobni podaci su se u putovnice unosili u policijskim upravama i postajama Ministarstva unutarnjih poslova te diplomatskim i konzularnim predstavništvima Republike Hrvatske u inozemstvu. Tadašnja hrvatska putovnica nije bila u skladu s međunarodnim standardima glede podataka koje je sadržavala, niti je bila strojno čitljiva.

Slika 1: Individualizacijska stranica prve hrvatske putovnice

[13] Zakon o putnim ispravama hrvatskih državljana. (NN 53/91., 64/92., 26/93. i 29/94.)

Iz navedenih je razloga, 1999. godine donesen novi Zakon o putnim ispravama hrvatskih državljana[14] koji je postavio pravni temelj za uvođenje novog tipa hrvatskih putovnica s čijim se izdavanjem započelo 1. siječnja 2000. godine. Navedene hrvatske putovnice bile su strojno čitljive i sukladne s tadašnjim međunarodnim standardima vezanima uz izgled, sadržaj i zaštitne elemente putnih isprava, propisanima od strane ICAO-a. Istodobno se pristupilo i centraliziranom postupku individualizacije putovnica. Zahtjev za izdavanje putovnice podnosio se ustrojstvenim jedinicama Ministarstva unutarnjih poslova prema mjestu prebivališta podnositelja zahtjeva, dok su hrvatski državljani koji nisu imali prebivalište u Republici Hrvatskoj, zahtjev za izdavanje putovnice mogli podnijeti nadležnoj diplomatskoj misiji ili konzularnom uredu Republike Hrvatske u inozemstvu. Spomenute su putovnice bile znatno zaštićenije u odnosu na prethodne, pa ih je samim time bilo i teže uspješno krivotvoriti.

Slika 2: Individualizacijska stranica hrvatske putovnice, izdavane u razdoblju od 1. 1. 2000. do 30. 6. 2009. godine

Slika 3: Prednje korice i individualizacijska stranica biometrijske e-putovnice Republike Hrvatske

Vodeći se aktualnim svjetskim i europskim trendovima u zaštiti putnih isprava, 2009. godine donijete su izmjene Zakona o putnim ispravama hrvatskih državljana[15]. Sukladno s time, nova elektronička putna isprava hrvatskih državljana mora sadržavati elektronički nosač podataka (RFID čip) na koji se pohranjuju ime i prezime, državljanstvo, datum rođenja, podatak o spolu, oznaka za vrstu putne isprave, oznaka države, broj putovnice,

[14] Zakon o putnim ispravama hrvatskih državljana. (NN 77/99., 133/02. i 48/05.)
[15] Izmjene Zakona o putnim ispravama hrvatskih državljana. (NN 74/09.)

osobni identifikacijski broj, datum izdavanja i datum isteka valjanosti putovnice, tijelo koje je putovnicu izdalo, fotografija i otisci prstiju. Podaci na elektroničkom nosaču podataka moraju se kriptološkim postupkom zaštititi od neovlaštenog čitanja, izmjene i brisanja. Postavljanjem pravnog okvira, Republika Hrvatska je 30. lipnja 2009. godine započela s izdavanjem nacionalnih biometrijskih e-putovnica *druge generacije* – elektroničkih putovnica s beskontaktnim čipom ugrađenim u strukturu polikarbonata na kojem su sadržane biometrijske karakteristike vlasnika putovnice – slika lica i otisci kažiprsta lijeve i desne ruke.

3. MEHANIZMI ZAŠTITE DIGITALNIH PODATAKA E-PUTOVNICA

Zaštita obrasca i vizualnog sadržaja putovnica implementiranjem različitih zaštitnih elemenata uvriježen je način zaštite od krivotvorenja koji državama primateljicama ujedno omogućava provjeru vjerodostojnosti putnih isprava. Uvođenjem biometrijskih e-putovnica javila se potreba za dodatnom zaštitom integriteta, autentičnosti i povjerljivosti digitalnih podataka pohranjenih na čipu e-putovnica. U tablici 2 prikazani su obvezatni i opcionalni mehanizmi zaštite digitalnih podataka pohranjenim na RFID čipu e-putovnica propisani od strane ICAO-a, kao i oni Europske unije, a vezani uz zaštitu digitalnih podataka u putovnicama tzv. *prve* i *druge generacije*.

MEHANIZAM ZAŠTITE	**ICAO**	**EUROPSKA UNIJA**		**SVRHA**
		prva generacija	***druga generacija***	
PASIVNA AUTENTIFIKACIJA	obvezatan	obvezatan	obvezatan	− zaštita autentičnosti i integriteta SO_D-a i logičke strukture podataka − ne sprječava kloniranje i izmjenu čipa, neovlašten pristup i *skimming*[16]
AKTIVNA AUTENTIFIKACIJA	opcionalan	obvezatan	obvezatan	− zaštita autentičnosti i integriteta čipa − ne sprječava prisluškivanje komunikacije između čipa i inspekcijskog sustava
OSNOVNA KONTROLA PRISTUPA	opcionalan	opcionalan	opcionalan	− zaštita od *skimminga* i prisluškivanja komunikacije između čipa i inspekcijskog sustava − ne sprječava kloniranje i izmjenu čipa
PROŠIRENA KONTROLA PRISTUPA	opcionalan	obvezatan	obvezatan	− zaštita od neovlaštenog pristupa otiscima prstiju, sprječava *skimming* otisaka prstiju − ne sprječava kopiranje i izmjenu čipa

Tablica 2: Obvezatni i opcionalni mehanizmi zaštite digitalnih podataka

[16] Pod pojmom *skimminga* podrazumijeva se krađa podataka, bilo magnetskih zapisa pohranjenih na magnetskim trakama, bilo digitalnih podataka pohranjenih na kontaktnim i beskontaktnim čipovima isprava.

3.1. Pasivna autentifikacija

Pasivna autentifikacija (eng. *Passive Authentication* – PA) je mehanizam zaštite autentičnosti i integriteta digitalnih podataka na čipu e-putovnica koji služi za provjeru autentičnosti i integriteta SO_D-a i logičke strukture podataka, no ne sprječava kloniranje, tj. kopiranje cjelokupnog sadržaja čipa ili izmjenu čipa, neovlašten pristup digitalnim podacima i tzv. *skimming.*

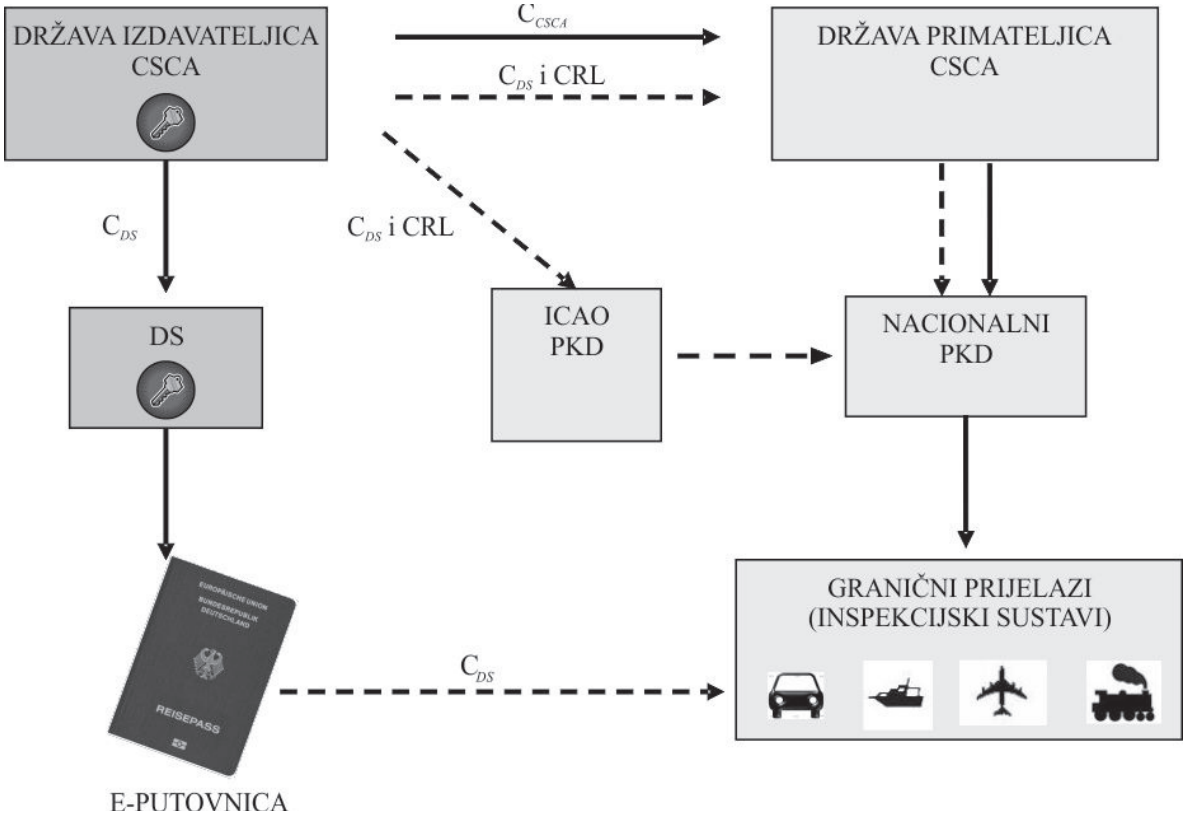
Protokol pasivne autentifikacije oslanja se na propisanu jedinstvenu shemu infrastrukture javnog ključa (eng. *Public Key Infrastructure* – PKI) koja omogućava nadležnim tijelima država primateljica provjeru autentičnosti i integriteta e-putovnica. Infrastruktura javnog ključa djeluje u potpuno ravnopravnom korisničkom okružju gdje je svaka država izdavateljica e-putovnica dužna ustanoviti nacionalnu infrastrukturu javnog ključa koja uključuje jedno krovno certifikacijsko tijelo države tzv. CSCA (eng. *Country Signing Certificate Authority*) odgovorno za potpisivanje i izdavanje certifikata, te barem jedno tijelo nadležno za izdavanje nacionalnih e-putovnica tzv. DS (eng. *Document Signer*), (ICAO, 2008).

Krovno certifikacijsko tijelo države izdaje glavni samopotpisan CSCA certifikat (C_{CSCA}) koji sadrži javni ključ (KPu_{CSCA}) i koristi se za provjeru autentičnost certifikata tijela nadležnog za izdavanje e-putovnica, tzv. DS certifikata (C_{DS}). Tajni ključ (KPr_{CSCA}) koristi se za potpisivanje DS certifikata i pohranjuje se u visokozaštićenom okružju države izdavateljice. Raspodjela C_{CSCA} državama primateljicama odvija se bilateralno, sigurnim diplomatskim sredstvima. Razdoblje valjanosti C_{CSCA}, koje je u pravilu tri do pet godina, utvrđuje se na osnovi razdoblja korištenja tajnog ključa (KPr_{CSCA}) za izdavanje DS certifikata i razdoblja valjanosti DS certifikata. Pri zamjeni CSCA ključeva, države izdavateljice moraju devedeset dana unaprijed najaviti izmjenu svog C_{CSCA} i nakon toga bilateralno raspodijeliti novi C_{CSCA}.

Krovno certifikacijsko tijelo države potpisuje i izdaje DS certifikat (C_{DS}) koji sadrži javni ključ (KPu_{DS}) i koristi se za provjeru autentičnosti i integriteta digitalnih podataka pohranjenih na čipu e-putovnice. Tajni ključ (KPr_{DS}) koristi se za potpisivanje SO_D-a i pohranjuje se u visokozaštićenom okružju države izdavateljice. Razdoblje valjanosti C_{DS}, koje je u pravilu tri mjeseca, utvrđuje se na osnovi razdoblja korištenja tajnog ključa (KPr_{DS}) za izdavanje putovnica i razdoblja valjanosti e-putovnica izdanih tim ključem, pri čemu C_{DS} treba biti valjan tijekom cjelokupnog razdoblja kako bi se državama primateljicama omogućila provjera autentičnosti e-putovnica. Država izdavateljica može C_{DS} raspodijeliti državama primateljicama bilateralno, sigurnim diplomatskim sredstvima ili putem Direktorija javnih ključeva (eng. *Public Key Directory* – PKD), ili ga pak može pohraniti u SO_D na čipu e-putovnice čime se olakšava postupak provjere autentičnosti i integriteta digitalnih podataka.

Osim toga, države izdavateljice dužne su periodično, u pravilu svakih 90 dana, objavljivati liste opozvanih certifikata (eng. *Certificate Revocation Lists* – CRL). Ukoliko država želi opozvati pojedini certifikat, na primjer u slučaju kompromitiranja tajnog ključa (KPr_{DS}), sastavlja obavijest o opozivu (eng. *CRL alert*) i unutar 48 sati objavljuje ažuriranu listu opozvanih certifikata koje bilateralnim, sigurnim diplomatskim sredstvima raspodjeljuje drugim državama. Pritom je potrebno napomenuti kako je opozivanje C_{CSCA}

ekstreman i složen postupak koji za sobom povlači i opoziv svih DS ključeva izdanih korištenjem tajnog ključa (KPr_{CSCA}).



Slika 4: Shematski prikaz ICAO infrastrukture javnog ključa

Države primateljice odgovorne su za raspodjelu C_{CSCA}, C_{DS} i listi opozvanih certifikata na nacionalnoj razini i za pohranjivanje C_{CSCA} države izdavateljice u visokozaštićenom okružju vlastitih inspekcijskih sustava granične kontrole.

U cilju pasivne autentifikacije, inspekcijski sustav države primateljice treba posjedovati znanje o C_{CSCA}, C_{DS} i listi opozvanih certifikata države izdavateljice e-putovnice. Pritom verifikacija certifikata od strane inspekcijskih sustava države primateljice podrazumijeva mnogostruke pristupe zapisima certifikacijskih tijela i listama opozvanih certifikata država izdavateljica u različitim bazama podataka, a što predstavlja složen postupak.

Protokol pasivne autentifikacije obavlja se na sljedeći način. Inspekcijski sustav iščitava SO_D s čipa e-putovnice. Iz odgovarajućih baza podataka povlači C_{CSCA}, C_{DS} (ili ga iščitava iz SO_D-a) i listu opozvanih certifikata. CSCA javnim ključem (Kpu_{CSCA}) verificira DS certifikat, nakon čega DS javnim ključem (KPu_{DS}) verificira digitalan potpis SO_D-a čime utvrđuje autentičnost i integritet SO_D-a. Potom, inspekcijski sustav iščitava relevantne skupine podataka unutar logičke strukture podataka i primjenjuje hash funkciju na skupine podataka. Dobivene *hash* vrijednosti uspoređuje s pripadajućim *hash* vrijednostima sadržanima u SO_D-u, čime verificira autentičnost i integritet skupina podataka unutar logičke strukture podataka (Nguyen, 2007).

3.2. Aktivna autentifikacija

Aktivna autentifikacija (eng. *Active Authentication* – AA) je mehanizam zaštite autentičnosti i integriteta čipa e-putovnice koji se temelji na tzv. *challenge-response* protokolu između inspekcijskog sustava i čipa. Aktivna autentifikacija služi za provjeru originalnosti čipa, no ne sprječava prisluškivanje komunikacije između inspekcijskog sustava i čipa. Za razliku od pasivne autentifikacije, protokol aktivne autentifikacije zahtijeva čip s mikroprocesorom.

U svrhu aktivne autentifikacije, čip posjeduje jedinstveni par ključeva za aktivnu autentifikaciju – tajni (KPr_{AA}) i javni ključ (KPu_{AA}). Javni ključ za aktivnu autentifikaciju služi za verifikaciju digitalnog potpisa i pohranjen je u skupini podataka 15 na čipu e-putovnice. *Hash* vrijednost javnog ključa sadržana je u SO_D-u i verificirana je kroz prethodnu pasivnu autentifikaciju. Pripadajući tajni ključ služi za generiranje digitalnog potpisa i pohranjuje se u zaštićenoj memoriji čipa.

Protokol aktivne autentifikacije odvija se na sljedeći način. Inspekcijski sustav optički iščitava strojno čitljivu zonu s individualizacijske stranice u putovnici i uspoređuje je s digitalnom strojno čitljivom zonom u skupini podataka 1, čime se potvrđuje povezanost individualizacijske stranica i čipa, odnosno da pripadaju istoj e-putovnici. Prethodno izvršenom, pasivnom autentifikacijom potvrđena je autentičnost i integritet SO_D-a, a time i digitalne strojno čitljive zone i javnog ključa za aktivnu autentifikaciju. Za provjeru autentičnosti i integriteta čipa, inspekcijski sustav u *challenge-response* protokolu s čipom koristi par ključeva za aktivnu autentifikaciju. Inspekcijski sustav iz skupine podataka 15 iščitava javni ključ za aktivnu autentifikaciju, nakon čega generira slučajan *challenge* kojeg šalje čipu. Čip digitalno potpisuje *challenge* i inspekcijskom sustavu šalje *response*. Inspekcijski sustav s pomoću javnog ključa verificira digitalan potpis, te u slučaju uspješne verifikacije inspekcijski sustav prepoznaje čip kao autentičan i neizmijenjen.

3.3. Osnovna kontrola pristupa

Osnovna kontrola pristupa (eng. *Basic Access Control* – BAC) je mehanizam zaštite povjerljivosti digitalnih podataka koji štiti od neovlaštenog pristupa podacima, sprječava tzv. *skimming* te umanjuje rizik od prisluškivanja komunikacije između inspekcijskog sustava i čipa uspostavljanjem zaštićenog komunikacijskog kanala.

Osnovna kontrola pristupa je simetričan protokol koji koristi dva ključa. U svrhu osnovne kontrole pristupa čip e-putovnice posjeduje jedinstvene ključeve za osnovni pristup putovnici – K_{ENC} za kriptiranje i K_{MAC} za provjeru autentičnosti poruke, koji su pohranjeni u zaštićenoj memoriji čipa. E-putovnica koja je zaštićena mehanizmom osnovne kontrole pristupa odbija pristup sadržaju čipa ukoliko inspekcijski sustav ne može dokazati da ima *fizički pristup* individualizacijskoj stranici e-putovnice. Dokaz se pruža kroz simetričan autentifikacijski protokol u kojem inspekcijski sustav dokazuje znanje o čipu jedinstvenim ključevima za osnovni pristup putovnici. Inspekcijski sustav ove ključeve generira iz podataka sadržanih u strojno čitljivoj zoni na individualizacijskoj stranici e-putovnice, tzv. *SČZ_info*, koja se sastoji od serijskog broja putovnice, datuma rođenja, datuma valjanosti putovnice i pripadajućih kontrolnih brojeva. Nakon uspješno izvršenog autentifikacijskog protokola, inspekcijski sustav i čip izvršavaju asimetričan

protokol razmjene ključeva gdje s pomoću ključeva za osnovni pristup putovnici generiraju jedinstvene ključeve sesije za uspostavljanje zaštićenog komunikacijskog kanala između čipa i inspekcijskog sustava, pa je njihova daljnja komunikacija zaštićena.

3.4. Proširena kontrola pristupa

Proširena kontrola pristupa (eng. *Extended Access Control* – EAC) predstavlja mehanizam zaštite autentičnosti, integriteta i povjerljivosti dodatnih biometrijskih značajki u e-putovnicama *druge generacije* – digitalnih otisaka prstiju. Proširena kontrola pristupa je skup protokola – protokol autentifikacije čipa i autentifikacije inspekcijskog sustava, koji zahtijevaju čip s mikroprocesorom minimalnog kapaciteta 64 kB (Karger, 2005).

Autentifikacija čipa (eng. *Chip Authentication* – CA) je protokol autentifikacije čipa u odnosu na inspekcijski sustav i svojevrsna je alternativa aktivnoj autentifikaciji navedenoj u ICAO specifikacijama jer se njome potvrđuje autentičnost i integritet čipa. Autentifikacija čipa ujedno poboljšava i mehanizam zaštite povjerljivosti podataka jer zamjenjuje kriptografski ključ osnovne kontrole pristupa s potpuno slučajnim ključem, čime se učinkovitije sprječava prisluškivanje komunikacije između inspekcijskog sustava i čipa. Autentifikacija čipa temelji se na asimetričnom protokolu razmjene ključeva. Javni ključ za autentifikaciju čipa i parametri domene pohranjeni su u skupini podataka 14, dok je pripadajući tajni ključ pohranjen u zaštićenoj memoriji čipa. Inspekcijski sustav iz skupine podataka 14 iščitava javni ključ i s pomoću parametara domene generira jednokratan par ključeva, od čega jednokratan javni ključ šalje čipu. Čip i inspekcijski sustav generiraju tzv. zajedničku tajnu (eng. *common secret*) iz koje izvode ključeve sesije za uspostavljanje zaštićenog komunikacijskog kanala. Novi ključevi sesije imaju veliku entropiju. Inspekcijski sustav, na osnovi činjenice da čip e-putovnice može koristiti nove ključeve sesije, zaključuje da je ključ korišten u protokolu autentičan.

Autentifikacija inspekcijskog sustava (eng. *Terminal Authentification* – TA) je asimetričan autentifikacijski protokol u kojem inspekcijski sustav dokazuje čipu da je ovlašten pristupiti osjetljivim biometrijskim značajkama pohranjenima na čipu. Pristup se odobrava kroz niz certifikata (eng. *certificate chain*), pri čemu isključivo država izdavateljica e-putovnice odlučuje o tome komu će odobriti pristup osjetljivim biometrijskim značajkama.

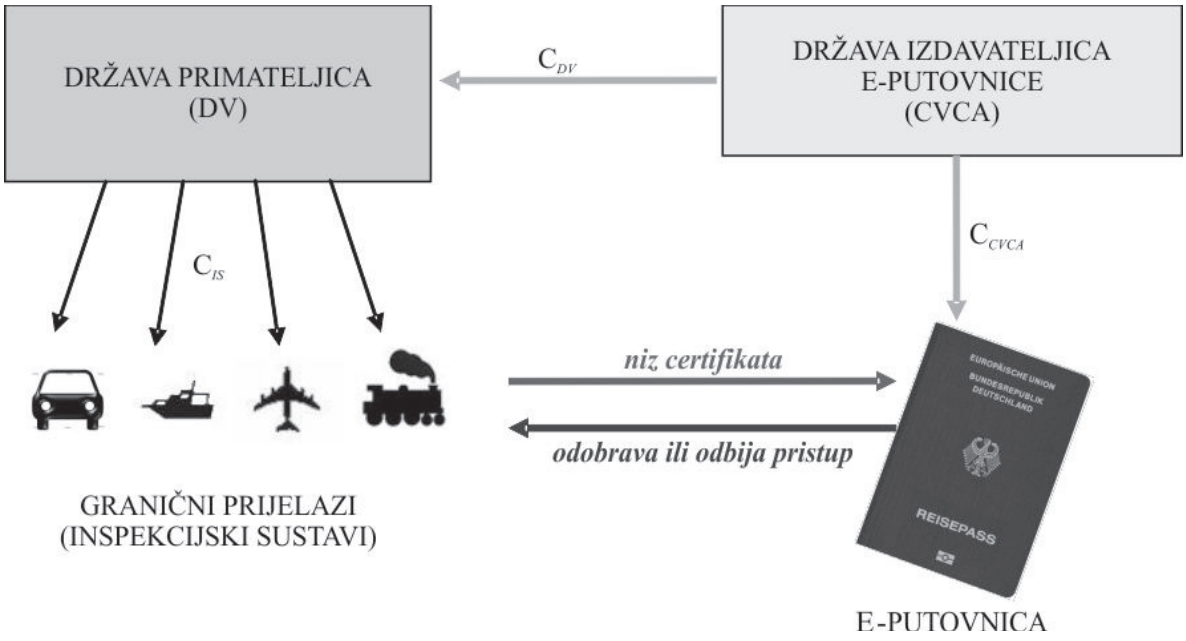
Protokol autentifikacije inspekcijskog sustava zahtijeva uvođenje dodatne infrastrukture javnog ključa i učinkovitu raspodjelu certifikata između država sudionica u cilju provođenja autentifikacije inspekcijskog sustava. S time u svezi, države trebaju ustanoviti jedno krovno certifikacijsko tijelo, tzv. CVCA (eng. *Country Verifying Certificate Authority)* i barem jedno tijelo nadležno za upravljanje nacionalnim inspekcijskim sustavima, tzv. DV (eng. *Document Verifier*).

Krovno certifikacijsko tijelo države izdaje glavni, samopotpisan CVCA certifikat (C_{CVCA}) koji se u postupku izrade e-putovnice pohranjuje u EF.CVCA na čipu. Osim toga, krovno certifikacijsko tijelo potpisuje i izdaje DV certifikate (C_{DV}) nacionalnim tijelima nadležnima za upravljanje inspekcijskim sustavima, ali i tijelima drugih država ukoliko im želi dopustiti pristup osjetljivim podacima pohranjenima na čipu u vlastitim e-putovnicama. C_{DV} sadržava razdoblje valjanosti certifikata, javni ključ i pravo pristupa digitalnim otiscima prstiju, odnosno informaciju o tome kojim osjetljivim podacima na

čipu pojedini DV ima ovlašten pristup. Radi smanjenja potencijalnog rizika u slučaju izgubljenih ili ukradenih inspekcijskih uređaja, C_{DV} ima kratko razdoblje valjanosti koje se može razlikovati ovisno o tijelu kojemu se certifikat izdaje. Tijelo nadležno za upravljanje nacionalnim inspekcijskim sustavima izdaje certifikate nacionalnim inspekcijskim sustavima (C_{IS}). Certifikat inspekcijskog sustava sadržava razdoblje valjanosti certifikata, javni ključ i pravo pristupa osjetljivim podacima za nacionalne e-putovnice. Pravo pristupa i razdoblje valjanosti C_{IS}-a u pravilu su jednaki onima C_{DV}-a, no DV može dodatno ograničiti pravo pristupa ili razdoblje valjanosti pojedinom inspekcijskom sustavu. Ukoliko država primateljica želi da inspekcijski sustavi u njezinoj nadležnosti imaju prava pristupa osjetljivim podacima e-putovnica drugih država, tijelo nadležno za upravljanje nacionalnim inspekcijskim sustavima mora zatražiti C_{DV} dotične države izdavateljice i osigurati njegovu raspodjelu vlastitim inspekcijskim sustavima.

Preporučljivo razdoblje valjanosti C_{CVCA}-a je šest mjeseci do tri godine, C_{DV}-a dva tjedna do tri mjeseca, a C_{IS}-a jedan dan do jedan mjesec. S obzirom na to da se CVCA par ključeva dosta često mijenja, uvedeni su i tzv. povezujući CVCA certifikati (eng. C_{CVCA} *link certificates*) koji služe za ažuriranje CVCA certifikata pohranjenog na čipu e-putovnice. Radi uspješne autentifikacije, inspekcijski sustav mora posjedovati znanje o povezujućim C_{CVCA}, DV certifikatu, te certifikatu inspekcijskog sustava i pripadajućeg tajnom ključu inspekcijskog sustava. Čip e-putovnice odobrava pristup inspekcijskom sustavu isključivo na osnovi prava pristupa sadržanih u sva tri certifikata.

Protokol autentifikacije čipa odvija se na sljedeći način: e-putovnica sadržava C_{CVCA} koji se pohranjuje na čip tijekom postupka proizvodnje e-isprave. Inspekcijski sustav, u cilju dokazivanja autentičnosti svog javnog ključa, predočava čipu niz certifikata – povezujuće C_{CVCA}, C_{DV} i C_{IS}. Sva komunikacija između čipa i inspekcijskog sustava zaštićena je još tijekom autentifikacije čipa uspostavljanjem zaštićenog komunikacijskog kanala. Nakon uspješne verifikacije niza certifikata, čip povlači javni ključ inspekcijskog sustava i šalje *challenge* inspekcijskom sustavu. Inspekcijski sustav s pomoću pripadajućeg tajnog ključa



Slika 5: Shematski prikaz dodatne infrastrukture javnog ključa

digitalno potpisuje *challenge* i šalje *response* čipu. Čip s pomoću javnog ključa inspekcijskog sustava provjerava autentičnost digitalnog potpisa inspekcijskog sustava. Ukoliko je autentifikacija inspekcijskog sustava uspješno izvršena, čip odobrava pristup osjetljivim podacima ovisno o razini autorizacije pojedinog inspekcijskog sustava (BSI, 2010).

4. SUSTAVI UPRAVLJANJA IDENTITETOM

Radi stvaranja pouzdanih sustava identifikacije i verifikacije osoba temeljenih na biometrijskoj tehnologiji, ponajprije je neophodno postojanje kvalitetnih i pouzdanih sustava upravljanja identitetom (eng. *Identity Management System*). Sustav upravljanja identitetom je mehanizam koji obuhvaća postupak inicijalnog utvrđivanja identiteta (identifikaciju), implementaciju, popratnu administraciju i postupak okončanja identiteta. Između ostaloga, takav sustav uključuje zakonodavni okvir, politiku, pravila i postupke, kao i skup koordiniranih aktivnosti. Svrha sustava je omogućavanje upravljanja identitetom na određenom području – na nacionalnoj i međunarodnoj razini. U osnovi, takvim se sustavom povezuju raznovrsni oblici identiteta s pojedinim subjektom, tvoreći cjelokupan identitet neke osobe. Sustavi upravljanja identitetom ne samo da olakšavaju vođenje registara građana, odnosno baza podataka na nacionalnoj razini, nego i pružaju mogućnost provjere identiteta, ažuriranje i korištenje biometrijskih karakteristika u razne, nacionalnim zakonodavstvima propisane svrhe (Broekhaar, 2011).

I dok s jedne strane postoje detaljno propisani međunarodni standardi vezani uz sadržaj, izgled, zaštitne elemente, implementaciju biometrijskih karakteristika i ostalih digitalnih podataka na čip, s druge strane, reguliranje samog postupka izdavanja e-putovnica ostavljeno je na nacionalnim zakonodavstvima država izdavateljica, pa ne čudi da se navedeni postupci razlikuju od države do države. Osim tehnološke usklađenosti putnih isprava po pitanju biometrijske tehnologije, neophodno je da se automatizirana provjera identiteta nositelja dokumenta zasniva na sigurnom i pouzdanom postupku prikupljanja i obrade podataka podnositelja zahtjeva za izdavanje isprava. Time uspješnost uvođenja e-putovnica na nacionalnoj razini uvelike ovisi o kvalitetnom sustavu upravljanja identitetom (Seidel, 2009).

Stoga, ukoliko već to nisu učinile, preporuča se da države u što skorije vrijeme uvedu središnje nacionalne registre državljana koji bi poslužiti i kao središnja baza podataka prilikom izdavanja identifikacijskih i putnih dokumenata. Naime, policijski službenici na graničnim prijelazima sve se češće susreću s osobama koje posjeduju dvije originalne putovnice, izdane na dva različita imena (dva identiteta : jedna osoba) od strane dviju država izdavateljica. Prema neslužbenim procjenama, tisuće osoba s dvostrukim ili višestrukim identitetom dnevno prelaze međunarodne granice služeći se originalnim putovnicama temeljenima na lažnom identitetu (Ruiter, 2011). Takve je zloporabe izuzetno teško otkriti zato što se radi o originalnim dokumentima izdanima od strane nadležnih tijela država izdavateljica, pri čemu je fotografija vlasnika dokumenta doista ona nositelja putne isprave. Identitet nositelja isprave ne odgovara identitetu osobe na čije je ime isprava izdana, no isprava je sama po sebi vjerodostojna, pa prilikom njezine provjere nije moguće utvrditi nikakve nepravilnosti. Ovakvi slučajevi ne samo da upućuju na neadekvatno upravljanje identitetom pojedinih država, nego i na nedostatak koordinacije na svjetskoj razini.

Stoga je ponajprije neophodno stvaranje središnjih, jedinstvenih registara državljana na nacionalnoj razini, čime bi se otvorila mogućnost njihova povezivanja na svjetskoj razini i umanjila mogućnost krađe identiteta, zloporaba identiteta, ilegalnih migracija, terorizma i ostalih oblika kriminaliteta.

Jedno je sigurno, pitanja vezana uz identitet zahtijevaju pozornost na svjetskoj razini. Jedan od najvećih izazova koji se postavlja pred države tiče se nacionalnih registara građana, poput registara rođenih i umrlih osoba, koji predstavljaju slabu točku sustava upravljanja identitetom, a za čiju implementaciju ne postoje međunarodno propisani minimalni standardi vezani uz sadržaj i format. Iako je često upravo rodni list isprava na osnovi koje se izdaju identifikacijski i putni dokumenti, on još i danas u većini zemalja predstavlja najslabiju kariku u lancu upravljanja identitetom. I bez obzira što se često postavlja pitanje pouzdanosti i vjerodostojnosti rodnih listova izdanih od strane afričkih zemalja, ne treba zanemariti ni činjenicu kako samo Sjedinjene Američke Države imaju preko 14 000 različitih tipova rodnih listova trenutačno u opticaju (Broekhaar, 2011).

5. RASPRAVA

Prednosti novih tehnologija poput beskontaktnog čipa s mikroprocesorom i biometrije pridobile su naklonost javnosti, no pitanja privatnosti i sigurnosti vezana uz uvođenje e-putovnica i dalje su ključna tema političkih i stručnih rasprava.

Najčešće postavljano pitanje vezano je uz mogućnost zloporabe biometrijskih značajki pohranjenih na čipu i narušavanja osobne privatnosti. Neki stručnjaci smatraju kako nema mjesta zabrinutosti jer je biometrijsku karakteristiku lica osobe, koja je odabrana kao primarna i obvezatna biometrijska značajka pohranjena u e-putovnicama *prve generacije*, moguće pribaviti i na druge jednostavnije načine, primjerice s pomoću fotoaparata ili kamere, pa stoga čitanje i korištenje biometrije lica s čipa ne bi trebalo izazivati zabrinutost javnosti, a i to je moguće jedino ukoliko je kompromitirana osnovna kontrola pristupa digitalnim podacima na čipu (Ellis, 2009). No istodobno treba napomenuti kako osnovna kontrola pristupa ne pruža odgovarajuću zaštitu povjerljivosti digitalnih podataka na čipu e-putovnica jer se simetrični ključevi za osnovni pristup putovnici ne generiraju iz slučajnog materijala, nego se izvode iz podataka sadržanih u strojno čitljivoj zoni na individualizacijskoj stranici e-putovnice i stoga posjeduju nedovoljnu entropiju. Sveukupna entropija tzv. *SČZ-info* manja je od 80 bita, odnosno one koju NIST (eng. *National Institute of Standards and Technology*) preporuča kao minimalnu zaštitu od prisluškivanja i drugih izvanmrežnih napada. Simetrični ključevi korišteni za uspostavljanje zaštićenog komunikacijskog kanala uspješno sprječavaju jednostavne *skimming* napade gdje tzv. napadač u prolazu pokušava iščitati digitalne podatke nositelja putovnice jer čip sporo odgovara na pojedini ključ. Međutim, čak i ICAO navodi da nedovoljna entropija osnovne kontrole pristupa omogućava napade grubom silom ili napade s pomoću rječnika (eng. *offline dictionary attacks*) ukoliko je napadač dulje vrijeme u blizini e-putovnice (Hoepman, 2011). Pojedine su se države, uključujući i Republiku Hrvatsku, odlučile za generiranje nasumičnog serijskog broja putovnice kako bi umanjile mogućnost takvih napada, no čak i takve e-putovnice posjeduju nedovoljnu entropija, približno 50 do 60 bita. Upravo iz toga razloga, ICAO i EU odlučile su mehanizam osnovne kontrole pristupa zamijeniti dodatnom

kontrolom pristupa (eng. *Supplemental Access Control*) koja se temelji na asimetričnoj kriptografiji i tzv. PACE protokolu[17], a koji je propisan kao obvezatan mehanizam zaštite e-putovnica tzv. *treće generacije* s čijim se izdavanjem započinje krajem prosinca 2014. godine (Bender, 2011).

Osim toga, sukladno s ICAO specifikacijama, jedini obvezan mehanizam zaštite digitalnih podataka – pasivna autentifikacija, sama po sebi ne pruža odgovarajuću zaštitu jer ne sprječava *skimming* i prisluškivanje komunikacije između čipa i inspekcijskog uređaja, niti jamči originalnost čipa (Karger, 2005).

Budući da biometrija lica ne predstavlja pouzdanu biometrijsku tehnologiju jer posjeduje relativno nizak stupanj jedinstvenosti, zloporaba tuđe e-putovnice *prve generacije* još je uvijek moguća. Osobe koje posjeduju slične fizičke karakteristike lica oduvijek su predstavljale problem za tijela granične policije – moguće je otuđiti nečiju putovnicu i prilagoditi vlastiti izgled kako se bi što više nalikovalo stvarnom vlasniku isprave (brada, brkovi, boja kose, itd.). Međutim, tradicionalne putovnice predstavljaju još veći problem jer je fotografija vlasnika na individualizacijskoj stranici malih dimenzija, što otežava raspoznavanje sličnih osoba. Nasuprot tome, e-putovnica sadrži digitalnu fotografiju visoke rezolucije koja se računalno može povećati, omogućavajući bolju usporedbu, a time i lakše raspoznavanje sličnih osoba. Korištenjem sustava za provjeru i raspoznavanje biometrije lica, još se više povećava vjerojatnost otkrivanja ovakvih oblika zloporaba. *Smartgate* sustav instaliran u zračnoj luci u Sydneyu, Australija, i slični sustavi u drugim državama poput Njemačke, Portugala i Velike Britanije omogućavaju softversku provjeru digitalne fotografije pohranjene na čipu e-putovnice s biometrijom lica nositelja putne isprave. Ukoliko se ne dobije potpuno podudaranje probnog i referentnog obrasca, provodi se dodatna provjera od strane policijskog službenika (Ellis, 2009).

Za razliku od biometrije lica, otisci prstiju ili šarenice oka smatraju se osjetljivijim biometrijskim podacima s aspekta privatnosti, pa ih je sukladno s time potrebno dodatno zaštititi. Krajem lipnja 2009. godine, zemlje članice Europske unije započele su s izdavanjem e-putovnica *druge generacije* čime se osigurala viša razina zaštite autentičnosti, integriteta i povjerljivosti digitalnih podataka pohranjenih na čipu e-putovnica. No ono što je potrebno naglasiti jest činjenica da se proširena kontrola pristupa uvodi isključivo na europskoj razini, dok na međunarodnoj razini nisu propisane detaljne specifikacije vezane uz zaštitu povjerljivosti osjetljivih biometrijskih značajki – otisaka prstiju i šarenice oka. Drugim riječima, odluka o tome hoće li nastaviti s izdavanjem e-putovnica *prve generacije* ili uvesti e-putovnice *druge generacije* ostavljena je u nadležnost pojedinoj državi izdavateljici. Osim toga, nedostatak međunarodnih specifikacija može imati za posljedicu uvođenje neodgovarajućih mehanizama zaštite osjetljivih biometrijskih podataka čime se ugrožava tajnost i privatnost osobnih podataka i otvaraju nove mogućnosti zloporabe (Hoepmann, 2011). Jednako tako, uvođenjem različitih, međusobno nekompatibilnih mehanizama zaštite osjetljivih biometrijskih značajki dovodi se u pitanje međunarodna interoperativnost – jedna od osnovnih svrha uvođenja e-putovnica. Ovdje je potrebno napomenuti kako je Republika Hrvatska odmah započela s izdavanjem e-putovnice *druge*

[17] PACE protokol (skraćeno od *Password Authenticated Connection Establishment*) razvijen je 2007. godine od strane BSI (German Federal Office for Information Security).

generacije čime se zaobišla većina ranije navedenih problema vezanih uz e-putovnice *prve generacije* i postigla viša razina sigurnosti elektroničke isprave.

Usporedno s uvođenjem e-putnih dokumenata, sve više država uvodi sustave za upravljanje državnom granicom koji omogućavaju automatiziranu provjeru elektronički čitljivih isprava na graničnim prijelazima. Međutim, osam godina nakon uvođenja elektroničkih putovnica, optimalna iskoristivost "e" u putnim ispravama tek treba uslijediti. Naime, provjera digitalnih podataka prilikom kontrole putnih dokumenata na graničnim prijelazima zasad još nije u potpunosti zaživjela uslijed nepostojanja razvijenih infrastruktura javnog ključa u pojedinim državama primateljicama, uhodane zajedničke certifikacijske politike, osobito za proširenu kontrolu pristupa, kao i zbog financijske i/ili tehnološke nemogućnosti implementacije automatiziranih sustava za upravljanje državnom granicom. Iz toga razloga, trenutačno mnogi granični prijelazi u svijetu nisu u mogućnosti pristupiti digitalnim podacima pohranjenima na čipu e-putovnica u svrhu identifikacije nositelja putovnice, te u osnovi čitaju samo strojno čitljivu zonu (Broekhaar, 2011).

U frankfurtskoj zračnoj luci svojedobno je provedeno testiranje e-putovnica koje je pokazalo da, iako je većina e-putovnica uspješno testirana, u otprilike 5 000 slučajeva CSCA certifikati nisu bili dostupni. Navedeno je testiranje također potvrdilo da temeljita i sveobuhvatna granična kontrola e-putovnica predstavlja imperativ. Naime, otkrivene su i dvije u cijelosti krivotvorene e-putovnice koje su sadržavale novi čip s parom ključeva za aktivnu autentifikaciju i digitalno potpisanim SO_D-om. Iako se čip na prvi pogled dojmio originalnim, pokazao se krivotvorenim pri pokušaju verifikacije DS certifikata s pomoću CSCA javnog ključa. U ovom slučaju, krivotvoreni čip ne bi bio otkriven da nije učinjena provjera i verifikacija svih potrebnih certifikata (Kinneging, 2009).

Što se tiče trenutačne situacije po pitanju sustava za upravljanje državnom granicom u Republici Hrvatskoj, Ministarstvo unutarnjih poslova uspješno je implementiralo osnovnu i dodatnu infrastrukturu javnog ključa čime je već sada omogućena automatizirana provjera e-putovnica *prve* i *druge generacije* na oko 80 graničnih prijelaza.

Još jedno aktualno pitanje vezano uz iskoristivost prednosti e-putnih isprava tiče se procedure u slučaju nemogućnosti pristupanja čipu, odnosno čitanja digitalnih podataka s njega. ICAO napominje kako se prema e-putovnicama s nefunkcionalnim čipom treba postupati kao i s ostalim zakonitim ispravama za prelazak državne granice, te da se nositelju takve putovnice neće zapriječiti ulazak u državu primateljicu isključivo na osnovi nefunkcionalnog čipa. No istodobno većina policijskih službenika na graničnim prijelazima preporučuje nositeljima takvih putovnica da ih što je to prije moguće zamijene. Nepotrebno je reći da će krivotvoritelji koji nisu u mogućnosti izmijeniti čip ili digitalne podatke na njemu, prije pokušati uništiti čip, negoli riskirati da budu otkriveni. Iz toga će se razloga morati uvesti stroža kontrola takvih e-putovnica u svrhu utvrđivanja eventualnih tragova namjernog onesposobljavanja RFID čipa. No pritom se neminovno nameće pitanje uspostavljanja ravnoteže između, s jedne strane, izbjegavanja nepotrebnog i kontraproduktivnog "kažnjavanja" ili zadržavanja legalnog nositelja putovnice zbog oštećenog ili neispravnog čipa u e-putovnici i, s druge strane, napora usmjerenih k otkrivanju beskrupuloznih činova namjerne sabotaže čipa od strane kriminalnih skupina (ICAO, 2008).

Na kraju, nikako ne treba zanemariti značaj uspostavljanja pouzdanih i sigurnih sustava upravljanja identitetom koji predstavljaju prvi i nezaobilazan korak ka stvaranju

učinkovitih sustava identifikacije i verifikacije osoba. Uvođenjem središnjih, jedinstvenih registara državljana na nacionalnoj razini otvara se mogućnost budućem povezivanju takvih registara na svjetskoj razini, a čime bi se zasigurno smanjila pojavnost krađa identiteta, zloporaba identiteta, ilegalnih migracija, terorizma i ostalih oblika kriminaliteta.

6. ZAKLJUČAK

Uvođenjem biometrije u e-putovnice, odnosno izdavanjem elektronski čitljivih putovnica s beskontaktnim RFID čipom za pohranu digitalnih podataka, ostvarena je dodatna zaštita dokumenta od krivotvorenja i učinkovitija verifikacija identiteta nositelja putovnice, a čime se osigurala viša razina sigurnosti međunarodnog kretanja osoba. U prilog općeprihvaćenosti implementacije biometrijske tehnologije u zaštićene dokumente govori i činjenica da se danas e-putovnice izdaju u više od osamdeset država diljem svijeta, s trenutačno oko 100 milijuna e-putovnica u opticaju, iako se s izdavanjem e-putovnica tzv. *prve generacije* započelo tek 2006. godine (Broekhaar, 2011).

I dok uvođenje biometrijskih e-putnih isprava predstavlja izniman korak na području zaštite dokumenata, nikako se ne smije zanemariti značaj tradicionalnih oblika zaštite koji i dalje ostaju ključan element cjelokupne sigurnosti isprave. Zaštitni su elementi učinkoviti jedino ukoliko ih se pravilno pregledava i provjerava. Isto se odnosi i na mehanizme zaštite digitalnih podataka u e-putovnicama – ukoliko inspekcijski sustav ne provede pravilnu, sveobuhvatnu provjeru, ove visokokvalitetne sigurnosne značajke postaju gotovo neučinkovite.

Iako pojedinci dovode u pitanje sigurnost RFID čipova u elektroničkim putovnicama, prema dosadašnjim saznanjima nije zabilježen niti jedan slučaj uspješnog kompromitiranja digitalnog potpisa (KP_{CSCA}) generiranog od strane države izdavateljice. No istodobno je potrebno istaknuti kako, sve dok su u opticaju putovnice tzv. *starog tipa* (bez ugrađenog RFID čipa), kriminalne će aktivnosti biti usmjerene na njihovo krivotvorenje ili zlouporabu, pa će stoga stvarne prednosti i nedostaci uvođenja e-putovnica doći do izražaja tek za otprilike pet godina.

Osim toga, iako su države uložile znatna sredstva u izradu visokozaštićenih elektroničkih isprava, uvodeći biometrijsku tehnologiju u identifikacijske i putne isprave koje na prvi pogled ulijevaju sigurnost, često se one, izravno ili neizravno, oslanjaju upravo na neadekvatne sustave upravljanja identitetom (Ruiter, 2011).

Uvođenjem biometrijskih e-putnih isprava ostvarena je dodatna zaštita dokumenta od krivotvorenja i učinkovitija verifikacija identiteta nositelja isprave, čime se osigurala viša razina sigurnosti međunarodnog kretanja osoba. No budući da je riječ o relativno novoj tehnologiji koja je još uvijek područje intenzivnog istraživanja, stvarne prednosti implementacije biometrijske tehnologije u zaštiti dokumenata tek imaju uslijediti.

LITERATURA

1. Bača, M. (2004). *Uvod u računalnu sigurnost*. Zagreb: Narodne novine.
2. Bender, J., Kügler, D. (2009*). Introducing the PACE solution: Countries need to be aware of the need to replace BAC*. Keesing Journal of Documents and Identity, 30, 26.-29.
3. Broekhaar, S., Wong, R. (2011). *Identity and Identity documents*. *Annual Report Identity Management 2010-2011.* Keesing Journal of Documents and Identity, 29.-36.
3. Broekhaar, S., Wong, R. (2011). *Identity management systems: A closer look at frameworks on a national and international level*. Annual Report Identity Management 2010-2011, Keesing Journal of Documents and Identity, 20.-23.
5. Broekhaar, S., Wong, R. (2011). *Results ICAO April 2010 deadline*. Annual Report Identity Management 2010-2011. Keesing Journal of Documents and Identity, 36.-41.
6. Broekhaar, S., Wong, R. (2011). *The unique human being: Human recognition systems draw on people's uniqueness*. Annual Report Identity Management 2010-2011. Keesing Journal of Documents and Identity, 5.-8.
7. Bundesamtes für Sicherheit in der Informationstechnik (2010). Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents, v 2.05. *https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html* - 10. 8. 2011.
8. Ellis, M. (2009). *39 myths about e-passports: The facts behind e-passport and RFID technology*. Keesing Journal of Documents and Identity, 30, 14.-23.
9. Grijpink, J. (2010). *Safe and Reliable use of biometrics*. Keesing Journal of Documents and Identity, 32, 7.-13.
10. Hartmann, M., Körting, S. (2009). *The ICAO PKD: Ten good reasons to join*. Keesing Journal of Documents and Identity, 30, 3.-6.
11. Hoepman, J. H., Hubbers, E., Jacobs, B., Oostdijk, M., Wichers Schreur, R. (2008). Crossing Borders: Security and Privacy Isues of the European e-Passport. *http://arxiv.org/PS_cache/arxiv/pdf/0801/0801.3930v1.pdf* - 10. 9. 2011.
12. Hornung, G. (2007). *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*. SCRIPTed − A Journal of Law, Technology & Society, 4(3), 246.-262.
13. ICAO (2008). *Document 9303, part 3, vol. 2*. 3 edit. Montreal: ICAO.
14. ICAO (2008). *Guidance to Border Control Authorities*. ICAO MRTD Report. Montreal: ICAO.
15. Karger, P. A. (2005). *ICAO RFI Response: Privacy-PreseRving Two-Way Authentication Protocol*. Montreal: Thomas J. Watson Research center, ICAO RFI.
16. Kinneging, T. (2009). *Inspecting the "e" in e-passports*. Keesing Journal of Documents and Identity. 28, 3.-7.
17. Nguyen, K. (2007). Contactless authentification protocols for MRTD. *http://www.iacr.org/workshops/ches/ches2007/presentations/I2-Nguyen.pdf* - 10. 8. 2011.
18. Nimac, L. (2007). Pregled biometrijskih metoda identifikacije. *http://os2.zemris.fer.hr/protokoli/2007_nimac/Seminar[2007]Nimac_Luka.html* - 10. 9. 2011.
19. Reisen, A. (2008). *Towards a multifunctional ID card: Germany progresses introduction of biometric ID card*. Keesing Journal of Documents and Identity, 27, 9.-11.

20. Ruiter, I. (2011). *ID Governance: Complexity demands coordination*. Annual Report Identity Management 2010-2011, Keesing Journal of Documents and Identity, 15.-19.
21. Seidel, U. (2009). *Fingerprint biometrics in e-passports*. Keesing Journal of Documents and Identity, 29, 3.-10.
22. Silicon Trust (2008). *Biometrics: Goverments face the future*. Keesing Journal of Documents and Identity, 27, 12.-16.

Summary

Jasminka Peroš, Gordan Mršić, Nevenka Škavić

The Deployment of Biometrics in Travel Documents

Taking into consideration a constantly increasing trend in counterfeited travel documents and misuse of genuine documents, which facilitate movement of terrorists and other criminal groups, international activities have been focused on harmonization of security mechanisms in travel documents, establishment of effective supervision over their issuance and control of persons and documents at border crossing points. In order to prevent such movements and contribute to overall security, specifications and recommendations concerning biometric deployment in e-passports have been laid down at international level. Biometric e-passports are machine readable travel documents which, besides visually and optically read characteristics, also contain biometric features of a bearer that are digitally stored on contacless IC chip within the passport. Advantages of implementing biometric e-passports, with respect to establishing a higher security in international movement of persons through additional identity verification, are beyond any doubt but at the same time privacy issues related to sensitive biometric identifiers stored on chip arise.

This article describes application of biometric technology in security of travel documents with emphasis on international, European and national legislation related to implementation of biometric electronic passports, security mechanisms used to ascertain the integrity, authenticity and privacy of digital data stored on chip in e-passports, as well as s significance of Identity Management Systems, that are closely related to the issues concerned.

Key words: biometrics, biometric e-passports, mechanisms for securing digital data, Public key infrastructure, Identity Management Systems.