Upotreba biometrijskih podataka i njihova međusobna razmjena u ID sistemima u BiH

Srđan Nogo, Siniša Macan
Agencija za identifikaciona dokumenta, evidenciju i razmjenu podataka BiH, Banja Luka, Bosna i Hercegovina
srdjan.nogo@iddeea.gov.ba , sinisa.macan@iddeea.gov.ba

Sadržaj— **Nakon što je uvela minimalne sigurnosne standarde za putne dokumente i pasoše država članica 2000.godine, Europska Unija-EU je nadogradila, standardizovala i harmonizovala minimalne sigurnosne stavke i uključila biometrijske uslove za pasoše i putne dokumente koje obavezuju Bosnu i Hercegovinu kada je u pitanju ova oblast i uspostavljanje bezviznog režima za njene državljane. Minimalni sigurnosni uslovi za putne dokumente i pasoše država odnose se na specifične materijale u upotrebi, mašinski čitljivu stranicu sa biografskim podacima, tehnikama štampanja, zaštiti od kopiranja, tehnikama izdavanja. U skladu sa standardima EU za biometrijske stavke, navodi da se oni moraju poklapati sa standardima predviđenim od strane International Civil Aviation Organizatio-ICAO. U ovome radu opisaćemo osnovne komponete sistema upotrebe biometrijskih podataka i njihova međusobna razmjena između nadležnih istitucija javne uprave u BiH.**

Ključne riječi: Radio-frequency identification (RFID), Standardi za uzimanje biometrijskih podataka,ICAO9303, Country Signing Certificate Authority- CSCA

I. UVOD

Uspostavljanjem Agencije za identifikaciona dokumenta, evidenciju i razmjenu podataka- IDDEEA na nivou BiH 2008 godine.osnovana je institucija koja prati, koordinira i institucionalno reguliše oblast identifikacionih dokumenata, koja u svom radu u okviru svojih zakonom definisanim nadležnostima teži zadovoljavanju relevantnih standarda i propisima Evropske unije.[1] Postojanje takve institucije omogućilo je da BiH uspostavi tehničke kapacitete koji se koriste za prenos podataka i međusobnu razmjenu između institucija na svim nivoima: Visoki sudski i tužilački savjet BiH (92 lokacije pravosudnih organa koriste mrežu Agencije IDDEEA za obavljanje svakodnevnih aktivnosti), 12 ministarstava unutrašnjih poslova (MUP Republike Srpske, MUP Federacije i 10 kantonalnih MUP-ova), 145 opština u Bosni i Hercegovini (Agencija IDDEEA je sprovela telekomunikacionu vezu prema matičnim službama tokom maja i juna 2009.), Javni registar Brčko distrikta, državna ministarstva i institucije (Ministarstvo civilnih poslova BiH, Ministarstvo inostranih poslova BiH), Centralna izborna komisija i Opštinska izborna komisija BiH, SIPA i Granična policija.

Pored resursa telekomunikacione mreže, više od 350 ustanova javne uprave u BiH na svim nivoima i više od 10 000 policajaca na 800 lokacija, koriste podatke iz resursa Agencije IDDEEA. Bez podrške koju pruža Agencija IDDEEA, kompletan sudski i tužilački, kao i policijski sistem u Bosni i Hercegovini našao bi se u blokadi. Postoji više od 160 miliona zapisa u elektronskom obliku u IDDEEA, iz čega proizilazi da je administrativna podrška IDDEEA potrebna svim vladinim administracijama u BiH. Pored toga, kompletni podaci o građanima Bosne i Hercegovine (putne isprave, Lične karte, prebivalište i boravište) kao i evidencije o vozilima, ličnim dokumentima i kaznama nalaze se u resursima Agencije IDDEEA. Vođenje takvih elektronskih evidencija kao i obezbeđivanje tehničkih kapaciteta za razmjenu podataka iz tih evidencija kroz pružanje Web Servisa-WS građanima i pravnom sektoru traži visok nivo fizičke i zakonodavne bezbjednosti.

Održavanje visokog nivoa sigurnosti elektronskih evidencija a samim time i biometrijskih podataka građana BiH koji isti sadrže od suštinskog su značaja za IDDEEA kako bi unaprijedila svoje unutrašnje kapacitete i bila spremna da preuzme obaveze koje proizilaze iz važećih bh. Zakona i propisa, a u skladu su sa Direktivom EU o usugama, čime bi se omogućila efikasnija saradnja i komunikacija sa građanima, poslovnom zajednicom i mnogim drugim javnim organizacionim jedinicama javne uprave u BiH na svim nivoima, koji na dnevnoj osnovi razmjenjuju informacije sadržane u elektronskim registrima koji su u nadležnosti Agencije. [2]

Bitno je spomenuti da se dva puta godišnje vrši monitoring institucija koje su bitne za provođenje aktivnosti koje za rezultat imaju ostanak BiH na bijeloj Šengen listi, kao i održavanje statusa bezviznog režima za BiH. Važna uloga Agencije IDDEEA u Bosni i Hercegovini i njena angažovanost u oblasti slobodnog viznog režima priznati su od strane eksperata Europske Unije- EU kroz pozitivne izvještaje koje podnose Evropskoj Komisiji u Briselu.

Takođe, Dom naroda Parlamentarne skupštine BiH jednoglasno je usvojio Zakon o izmjenama i dopunama Zakona o ličnoj karti državljana BiH, koji predstavlja osnovni preduslov da 2013. Godine počne izdavanje novih ličnih karata sa elektronskim čipom e-ID koji će sadržavati biometrijske podatke i digitalni potpis. [3] Uvođenjem e- ID lične karte stvoriće preduslove da se poveća broj pružanje WS usluga građanima kroz web portale kojima raspolažu javne institucije u BiH.

II. TRENUTNO STANJE MEĐUSOBNE RAZMJENE PODATAKA IZMEĐU INSTITUCIJA JAVNE UPRAVE U BiH

Javna uprava u BiH pruža usluge građanima u 146 opština, 2 entiteta, Brčko Distriktu i na državnom nivou. Na svakom nivou postoje različiti problemi koji su uključeni u funkcionisanje javne uprave. Principi i prakse na nivou opštine ili kantona razlikuju se od principa usvojenih u drugoj opštini, kantonu ili BiH. [5] Trenutno stanje na svim nivoima javne uprave u Bosni i Hercegovini ukazuje na to da postoji nedostatak razumijevanja značaja elektronske tehnologije koja bi se mogla uključiti u funkcionisanje javne uprave. Uvođenjem elektronske vlade u javnu upravu u Bosni i Hercegovini se uglavnom smatra kompjuterizacija određenih poslovnih procesa, a onda sredstvom za reformu javne uprave. Postoji nedostatak transparentnosti kada se radio o poslovnim i finansijskim pitanjima. Ne postoji ni horizontalna, niti vertikalna elektronska komunikacija. Službe javne uprave koriste različite operativne sisteme, aplikacije i baze podataka sistema zbog nedostatka standarda i nema globalnog plana za uvođenje informacionih tehnologija u državnu upravu. Vebsajtovi organa javne uprave ne pružaju građanima mnogo usluga, rijetko ažuriraju informacije i rijetko sadrže obrasce koji se mogu štampati na lokalnom nivou [4].

Tehničke mogućnosti administrativnih jedinica su donekle zadovoljavajući. Veliki broj lokalnih pravnih i administrativnih organizacija pravilno je tehnički pripremljeno i imaju kvalitetnu informatičku opremu. Međutim, oprema se često ne koristi na odgovarajući i zadovoljavajući način i u skladu sa propisima i procedurama, koje su uspostavile nadležne institucije. 55% zaposlenih u administraciji zna da koristi računar, ali je samo 5% stručnog IT osoblja zaposleno u IT ili ekvivalentnom sektoru. Nedostaje konstantna upotreba internet tehnologija. Postoji formalno prisustvo elektronske uprave na internetu samo na nekoliko opštinskih, entitetskih ili državnih vebsajtova, koji se koriste kao zvanični izvori informacija. Ove stranice pružaju korisnicima statične podatke o vladinim institucijama, sektorima, ministarstvima, agencijama i sl, kao i kontakt informacije, ali uglavnom im nedostaje aktuelnosti podataka. Jedan projekat koji je uspješno implementiran je Projekat za potrebe opština za izdavanje izvoda iz matične knjige rođenih i uvjerenja o državljanstvu za potrebe izdavanja biometrijskih pasoša. Korišćenje ovih veb rješenja je značajno skratilo redove u opštinama i smanjilo pritisak na referente. [5]

Problem verifikacije ulaznih dokumenata u procesu izdavanja ličnih dokumenata (izdavanje putne isprave) je prepoznat kao najslabija karika sistema. Relevantna iskustva širom svijeta su jednaka onima u BiH. Agencija pokušava da podigne nivo kvaliteta rada u ovoj oblasti na što viši nivo kako bi uskladili proces izdavanja dokumenata sa evropskim standardima [6]. Zakon o putnim ispravama ne nameće obavezu da pojedinac koji poseduje identifikacioni dokument mora da podnese zahtjev za izdavanje putne isprave uz rodni list i uvjerenje o državljanstvu. Pretpostavlja se da će se provjera te vrste sprovoditi u toku postupka izdavanja lične karte. Nažalost, očigledno je da je raniji proces prije uvođenja novih procedura izdavanja ličnih karata imao niz slabosti, prije svega u oblasti ulaznih dokumenata. Dakle, samo ti podaci koji se tada trenutno nalazili u registru građana ne mogu se uzeti kao apsolutno tačni. Nivo sigurnosti povećan je konstantnom internom i eksternom kontrolom kao I održavanjem nivoa poštovanja procedura od strane referenata koji rade na lokacijama koje služe za prikupljanje biometrijskih i drugih podataka kada je u pitanju izdavanje ličnih dokumenata u BiH. [19]

Zahvaljujući Projektu upravne odgovornosti - GAP, 70 opština na teritoriji BiH je postalo dio jedinstvenog informacionog sistema. Kroz implementaciju ovog sistema, pored ispunjavanja uslova da se uvede sistem biometrijskih putnih isprava, opštine su dobile odgovarajuće infrastrukturne mreže, kao osnovni uslov za uspostavljanje opštinskih informacionih sistema za: elektronski registar, razmjenu podataka između opština, elektronsku vladu, infrastrukturu javnog ključa (PKI), verifikaciju elektronskim potpisom, itd. [5]

Zbog nebrige institucija za lokalnu upravu, kao i neinformisanosti i slabe svijesti u vezi sa procesom vezanim za ispunjavanje uslova u cilju pristupanja EU, finansiranje i realizacija ovog projekta u svim lokalnim zajednicama u BiH nije moguća u razumnom vremenskom periodu. Naravno, postoje opštine koje će zadovoljiti potrebne uslove kao što je navedeno od strane EU standarda i procedura, ali je još izvjesnije da postoje opštine gdje će takav proces nerazumno dugo trajati.

Odgovori na pitanja o posjedovanju elektronskih registara, postojanje lokalnih mreža, položaj izbornih opštinskih komisija (IOK), itd. iz svih opština u BiH obezbijeđeni su u saradnji sa GAP-om. Dobijeni podaci potvrđuju da 67% opština već imaju elektronske registre i da su 83% opština već ispunile tehničke uslove za pristup informacionom sistemu IDDEEA. [5]

III. STANDARDI

U kontekstu međunarodnih standarda u oblasti identifikacionih dokumenata, potrebno je izdvojiti ICAO standarde. ICAO je specijalna međunarodna agencija Ujedinjenih Nacija-UN za civilni avionski saobraćaj koja je osnovana 1944. godine u Čikagu, potpisivanjem Konvencije o međunarodnoj civilnoj avijaciji. [7]

U skladu sa ovim mandatom, ICAO razvija i održava međunarodne standarde u aneksu IX – Upravljanje prema čikaškoj konvenciji za implementaciju od država potpisnica. U razvoju takvih standarda, osnovni princip je da ukoliko će javne vlasti vršiti kontrole, moraju da imaju zadovoljavajući nivo povjerenja u pouzdanost putnih dokumenata i u efektivnost inspekcijskih procedura. Izrada stadardizovanih specifikacija za putne dokumente i podatke koje se u njih postavljaju služi za izgradnju tog povjerenja.

Skupština ICAO je u 2004. godini potvrdila da saradnja na specifikacijama za jačanje sigurnosti i integriteta putnih dokumenata treba biti nastavljena kao stvar od velike važnosti za organizaciju. Pored Međunarodne ogranizacije za standardizaciju- ISO, konsultanti ICAO-a su uključili i Međunarodnu asocijaciju zračnog transporta- IATA , Međunarodno vijeće aerodroma ACI kao i Međunarodnu policijsku organizaciju za kriminal - INTERPOL.[8] U 2005. godini tadašnjih 188 zemalja potpisnica ICAO-a su odobrile

novi standard da svi moraju početi izdavati mašinski čitljive pasoše u skladu sa Dokumentom 9303, i to ne kasnije od 2010. godine. [9]

Iskustvo sa izdavanjem mašinski čitljivih pasoša, u skladu sa specifikacijama postavljenim Dokumentom 9303, ukazuje na to da troškovi izdavanja mašinski čitljivih pasoša ne mogu biti veći od izdavanja konvencionalnih dokumenata, iako će troškovi porasti implementacijom biometrije i pohranjivanjem elektronskih podataka na dokumentu. Kako se promet povećava i više zemalja se fokusira kako da racionalizuju svoje procedure prelaska granica sa upotrebom elektronskih baza podataka i međusobnom razmjenom podataka iz elektronskih baza podataka, mašinski čitljivi putni dokumenti igraju ključnu ulogu u najnovijem, unaprijeđenom usklađenom sistemu. Oprema za čitanje dokumenata i pristup bazama podataka mogu zahtijevati značajnu novčanu investiciju , ali se takođe može očekivati da će to brzo biti vraćeno kroz povećanu sigurnost, brzinu prelaska granica i tačnost verifikacije što ovi sistemi pružaju. Upotreba mašinski čitljivih putnih dokumenata u automatskom sistemu prelaska, može takođe omogućiti državama da eliminišu potrebu za papirnim dokumentima u proces prelaska granice, kao i administrativne troškove u vezi tih manuelnih procedura. [10]

Tehnički dio dokumenta 9303 je dobio potvrdu i od strane Međunarodne organizacije za standardizaciju kao ISO standardi 7501-1, 7501-2 i 7501-3. Takva potvrda je moguća zahvaljujući sredstvima povezanih mehanizama putem kojih proizvođači putnih dokumenata, čitača i ostale tehnologije pružaju tehničke i druge savjete ICAO-u pod okriljem ISO-a. Preko ove radne veze, ICAO specifikacije su postigle status svjetskih standarda putem pojednostavljene procedure u okviru ISO. [11]

ICAO svojim dokumentom ICAO 9303 definiše standarde u oblasti identifikacionih dokumenata i u Bosni i Hercegovini. Zakonom o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka BiH, propisano je da Agencija predlaže i provodi strategiju i politiku razvoja u Bosni i Hercegovini u oblasti identifikacionih dokumenata, a prema ICAO 9303 standardu i drugim relevantnim standardima. ICAO ima odlučujući uticaj na tehničke aspekte biometrije koja se koristi u pasošima i putničkim dokumentima. Dokument 9303 je smjernica koje se legalno implementira i od strane EU zakonodavstva. Evropska unija je svojim propisima uputila na dokument 9303 i obaveznu upotrebu Radio-frequency identification - RFID čipa. [12]

Globalno, ICAO-ov Dokument 9303 je usvojen kao standard za nove e-pasoše. Usvajanjem globalnih standarda, svi pasoši bi trebalo da su interoperabilni između regiona i država.

Za razliku od tradicionalnih pasoša, standard propisuje upotrebu mikročipa ugrađenog u plastičnu karticu u papirnom pasošu i bezkontaktnog mehanizma za razmjenu podataka.

A. Regulativa Evropske Unije

Iako države članice Evropske Unije već izdaju pasoše za biometrijom, EU trenutno ide ka dalekosežnom razvoju biometrijskih pasoša i putnih dokumenata za EU građane tzv. Evropskom pasošu.

Nakon što je uvela minimalne sigurnosne standarde za putne dokumente i pasoše država članica 2000.godine, EU je nadogradila, standardizovala, i harmonizirala minimalne sigurnosne stavke i uključila biometrijske uslove za pasoše i putne. Minimalni sigurnosni uslovi za putne dokumente i pasoše država članica odnose se na specifične materijale u upotrebi, mašinski čitljivu stranicu sa biografskim podacima, tehnikama štampanja, zaštiti od kopiranja, tehnikama izdavanja. U skladu sa standardima za biometrijske stavke, Uredba 2252/2004 navodi da se oni moraju poklapati sa standardima predviđenim od strane ICAO-a u ICAO Dokumentu 9303. [10]

Biometrija za pasoše i putne dokumente je uvedena ovom Uredbom sa ciljem da učini putne dokumente sigurnijim i da uspostavi pouzdaniju vezu između nosioca pasoša i putnog dokumenta. Prema tome, upotreba biometrije cilja na verifikaciju validnosti pretpostavljenog identitita umjesto uspostavljanje identitita osobe. Glavne karakteristike Uredbe su:

a) Slika lica i otisak prsta smješteni na RFID čipu;

b) Svrha upotrebe biometrijskih stavki u verifikaciji autentičnosti dokumenta i identiteta nosioca;

c) Prava subjekata čiji se podaci pohranjuju;

d) Ograničena upotreba i implementacija.

Ograničena upotreba i implementacija Uredbe je ta da se ne primjenjuje na nacionalne lične karte ili privremene pasoše i privremene putne dokumente koji imaju rok važenja od 12 mjeseci ili manje. [12]

Okvir harmonizacije je takođe ograničen sigurnosnim stavkama: određivanje tijela i nadležnosti kojima će biti dozvoljen pristup podacima koji su smješteni na izdatom dokumentu, ostaju pitanje nacionalne legislative. Države članice su trebale da implementiraju digitalnu sliku lica u pasoše prije 28. avgusta 2006, a otisaka prstiju prije 28. Februara 2008. [13]

Svrha donošenja novih dopunjenih Uredbi sa ciljem da se definišu izuzeci za davanje otisaka prstiju za djecu ispod 12 godina i određenih osoba koje nisu u stanju fizički da daju otiske prstiju za putne dokumente a što nije bilo predviđeno Uredbom 2252/2004. Tamo gdje je davanje otiska prstiju privremeno nemoguće, države članice će uzeti otiske prstiju ostalih prsta, a gdje je i to nemoguće, može se izdati privremeni pasoš trajanja od 12 mjeseci ili manje. Harmonizacija izuzetaka od generalne obaveze da se daju otisci prstiju je ključna radi održavanja zajedničkih sigurnosnih standarda i sa ciljem pojednostavljenja graničnih kontrola.

Starosna granica od 12 godina je provizorna, a Komisija će do 26 juna 2012 godine dati izvještaj povodom ovog pitanja, i ako je neophodno predložiti reviziju starosne granice.

Države članice, ukoliko njihovi nacionalni zakoni usvojeni prije 26. juna 2009.godine, dozvoljavaju starosnu granicu ispod

12 godina, mogu ovo pravilo primjenjivati tijekom tranzicijskog perioda do 26. juna 2013. godine. Međutim, starosna granica ni u tranzicijskom periodu ne smije biti ispod 6 godina. Uredba takođe uvodi u skladu sa preporukom ICAO-a princip "jedna osoba – jedan pasoš" sa ciljem da se uspostavi sigurnije veza između nosioca pasoša i putnog dokumenta. Uredba propisuje različitu aplikaciju u skladu sa integracijom tehničkih specifikacija. U principu, uspostava biometrijskog pasoša će se odvijati do 26. juna 2012. godine, ukoliko nije drugačije navedeno. U svakom slučaju, validnost prethodno izdatih pasoša i putnih dokumenata neće biti sporna. [13]

IV. SADRŽAJ ELEKTRONSKOG MEMORIJSKOG ELEMENTA PUTNIH ISPRAVA BOSNE I HERCEGOVINE

U ovome poglavlju opisaćemo operativni sistem elektronskog memorijskog elementa putnih isprava BiH, način zaštite podataka na elektronskom memorijskom elementu putnih isprava BiH, sadržaj elektronskog memorijskog elementa putnih isprava Bosne i Hercegovine i način izdavanja i zamjene certifikata sadržanih u elektronskom memorijskom elementu putnih isprava Bosne i Hercegovine.

Obrazac biometrijske putne isprave Bosne i Hercegovine sadrži elektronski memorijski element proizvođača NXP pod oznakom P5CD080A4.

Elektronski memorijski element putnih isprava Bosne i Hercegovine sadrži operativni sistem Telesec Chipcard Operating System (TCOS) V2R2 - verzija dva, podverzija dva. [14]

Vrste kontrole pristupa: Podaci na elektronskom memorijskom elementu štite se pomoću dvije vrste kontrole pristupa:

a) osnovna kontrola pristupa (Basic Access Control - BAC) i

b) proširena kontrola pristupa (Extended Access Control - EAC).

Osnovna kontrola pristupa bazira se na generiranju simetričnog ključa za pristup dijelovima sistema datoteka na osnovu podataka iz mašinski čitljive zone. Osnovna kontrola pristupa koristi se za pristup fotografiji smještenoj u elektronskom memorijskom elementu. [15]

Proširena kontrola pristupa bazira se na upotrebi postupka za predstavljanje elektronskog memorijskog elementa (Chip Authentication - CA) i predstavljanje uređaja za čitanje elektronskog memorijskog elementa. (Terminal Authentication -TA). [16] Koriste se složeni kriptografski postupci bazirani na eliptičnim krivama. Primjeno ovog kontrolnog pristupa zaštićeni su otisci prstiju. Od 01.06.2011 godine IDDEEA je počela sa upotrebom proširene kontrole pristupa i personalizacijom putnih isprava sa EAC kontrolom pristupa. [15]

A. Sistemi datoteka

TCOS operativni sistem omogućava upravljanje sistemom datoteka u skaldu sa standardom ISO 7816-4. Sistem datoteka se sastoji od „dedicated files" - fascikla i „elementary files" - osnovnih datoteka. Fascikla DF1 sadrži sve osnovne datoteke potrebne za rad pasoške aplikacije. [15]

(1) Osnovne datoteke (EF) sadržane u fascikli pasoške aplikacije (DF1) su:

a) EF.SOD - sadrži heš vrijednosti upotrijebljenih osnovnih datoteka u zavisnosti od upotrijebljene kontrole pristupa. Kao heš funkcija koristi se SHA-1,

b) EF.COM - sadrži listu iskorištenih osnovnih datotetka u zavisnosti od upotrijebljene kontrole pristupa,

c) EF.LDO - sadrži serijski broj obrasca putne isprave kodiran za potrebe predstavljanja uređaja za čitanje elektronskog memorijskog elementa,

d) EF.GDO - sadrži serijski broj obrasca putne isprave

e) EF.DP - sadrži parametre eliptične krive brainpoolp256r1 korištene za potrebe predstavljanja elektronskog memorijskog elementa u procesu uspostavljanja proširene kontrole pristupa,

f) EF.KEY1 - sadrži simetrični ključ za otvaranje elektronskog memorijskog elementa u procesu osnovne kontrole pristupa i privatni ključ generisan upotrebom ECDH generatora za potrebe predstavljanja elektronskog memorijskog elementa,

g) EF.CVCA - sadrži root CVCA certifikat neophodan za verifikaciju DV i IS certifikata uređaja za čitanje elektronskog memorijskog elementa u procesu proširene kontrole pristupa,

h) EF.DG1 - sadrži mašinski čitljivu zonu,

i) EF.DG2 - sadrži fotografiju lica nosioca putne isprave u JPEG formatu,

j) EF.DG3 - sadrži dva otiska prsta lica nosioca putne isprave zapisane u WSQ ili JPEG formatu,

k) EF.DG12 - sadrži dodatne podatke o samom dokumentu putne isprave - nadležni organ, serijski broj printera, datum i vrijeme personalizacije, datum izdavanja i napomenu,

l) EF.DG13 - sadrži podatke o službenom licu koje je izvršilo akviziciju podatka za putne isprave koje ne sadrže otiske prsta i ime i prezime nosioca putne

isprave,

m) EF.DG14 - sadrži javni ključ generiran upotrebom ECDH generatora za potrebe predstavljanja elektronskog memorijskog elementa.

(2) Za potrebe osnovne kontrole pristupa popunjavaju se osnovne datoteke: a), b), d), h), i i). Za potrebe proširene kontrole pristupa popunjavaju se dodatno i preostale osnovne datoteke: c), e), f), g), j), k), l) i m). [15]

B. Certifikati

(1) IDDEEA predstavlja CSCA (Country Signing Certificate Authority) i izdaje CS certifikat. To je ECDSA sa SHA-1 certifikat koji se koristi za izdavanje DS (Document Signer) certifikata.

(2) U skladu sa preporukama ICAO-a CSCA certifikat se izdaje sa rokom važnosti od 10 godina i 3 mjeseca. Važnost privatnog ključa za potpisivanje certifikata je 5 godina.

(1) DS certifikat je certifikat kojim Agencija, kao nadležni organ u BiH, vrši potpisivanje osnovne datoteke EF.SOD čime dokazuje autentičnost putne isprave. Ovaj certifikat potpisan je sa CSCA privatnim ključem i može se provjeriti korištenjem javnog CSCA ključa. [15]

(2) U skladu sa preporukama ICAO-a DS certifikat će se izdavati sa rokom važnosti od 5 godina i 3 mjeseca. Važnost privatnog ključa za potpisivanje EF.SOD osnovne datoteke je 3 mjeseca.

Javni ključ CSCA certifikat je dostupan za druge učesnike u sistemu razmjene certifikata za provjeru validnosti biometrijske putne isprave putem „web" stranice Agencije. [16]

(1) Agencija je nadležni organ za izdavanje DV (Document Verifiers) certifikata i kao takva predstavlja CVCA (Country Verifying Certificate Authority).

(2) CV (Country Verifying) certifikat je samopotpisani certifikat u skladu sa ISO 7816 izdat od strane Agencije na rok od 5 godina i četiri mjeseca. Mijenja se svakih 5 godina. CV certifikate za potpisivanje koristi ECDSA algoritam, a za izračunavanje heša algoritam SHA-256.

(3) DV certifikat koji Centar za skladištenje, personalizaciju i transport ličnih dokumenata, kao organizaciona jedinica Agencije koja vrši personalizaciju dokumenata, koristi za izdavanje certifikata za uređaje za kontrolu kvaliteta putnih isprava, mijenja se svaka 3 mjeseca.

(4) Certifikati za uređaje za kontrolu kvaliteta putnih isprava se također izdaju na rok od tri mjeseca.

Agencija, kao nadležni organ za personalizaciju putnih isprava, predstavlja centralnu tačku za razmjenu podataka (Single Point Of Contact) sa drugim državama koje žele da vrše kontrolu izdatih putnih isprava Bosne i Hercegovine. Agencija je dužna da u skladu sa međunarodnim propisima i potpisanim bilateralnim ugovorima vrši izdavanje DV certifikata za druge zemlje. Također, dužna je da prikuplja zahtjeve domaćih institucija i vrši proslijeđivanje istih prema odgovarajućem organu zemlje za čije putne isprave je zahtijevan DV certifikat. [15]

V. ZAKLJUČAK

Uspostavljanjem Agencije IDDEEA na nivou BiH, stvorena je institucija koja prati, koordiniše i institucionalno uređuje oblast identifikacionih dokumenata, slijedi odgovarajuće standarde i propise Evropske unije i ICAO standard kao i razvoj u skladu sa tim standardima. Postojanjem jedne takve institucije koja kordiniše prikupljanje, akviziciju, personalizaciju i razmjenu podataka za potrebe ID sistema, stvorili su se uslovi da BiH zadovoljavanjem Evropskih standarda iz ove oblasti bude uvrštena na Bijelu šengen listu. Ako se sagleda stanje u BiH dolazimo do zaključka da je BiH u veoma uspješna kada je upotreba biometrijskih podataka građana u memorijskim elementima putnih isprava u pitanju. Mnogi projekti koji se implementiraju u svijetu koji koriste biometrijske tehnologije dokazali su u praksi da su dosegli veoma visok stepen tehnološkog napredka u ovoj oblasti ali sa tendencijom stalnog poboljšanja koji digtiraju pojave novih sofisticiranijih tehnologija i alata za uzimanje biometrijskih podataka. Ipak slučaj BiH pokazuje da se za razumnu finasijsku konstrukciju za zemlju koja je potencijalni kandidata za članstvo u EU u poređenju sa zemljama EU koji imaju približno jednak broj stanovnika kao i BiH može razviti sistem koji zadovoljava sve tehničke standarde koje jedna zemlja treba imati kada su u pitanju ID informacioni sistemi.

LITERATURA

[1] Zakon o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine ("Službeni glasnik BiH", broj 56/08).

[2] The EU Services Directive (Directive 2006/123/EG) of 12 December 2006

[3] Zakon o izmjenama i dopunama Zakona o ličnoj karti državljana Bosne i Hercegovine, Usvojen u Domu naroda: 29.2.2012. 13. sjednica Doma naroda Parlamentarne skupštine BiH, Broj Službenog glasnika BiH: 18/12,https://www.parlament.ba/sadrzaj/zakonodavstvo/u_procedure/default.aspx?id=29009&langTag=bs-BA&pril=b,(preuzeto: 30.01.2012.)

[4] S. Gerin, B. Vujičić, "Usluge elektronske vlade u Bosni i Hercegovini", Informatica, 31, 1, str. 373-377, 2007.

[5] Leonid Stoimenov, Nataša Veljković, Sanja Bogdanović-Dinić, Srđan Nogo and Siniša Macan, Development of e-Government in Serbia and Bosnia and Herzegovina, ICEST 2010, Conference, Ohrid 2010, Macedonia.

[6] M. Gusev, G. Armenski "Analiza nedostataka elektronske vlade u zemljama zapadnog Balkana", vvv.metamorphosis.org.mk, 2006.

[7] http://www.aviation.go.th/airtrans/airlaw/chicago.html- Konvencija o međunarodnoj civilnoj avijaciji (pregledano: 03.03.2012.)

[8] http://www.iata.org/Pages/default.aspx- Međunarodna asocijacija zračnog transporta(pregledano: 03.03.2012.)

[9] http://www.interpol.int/contentinterpol/search?SearchText=ICAO&x=0&y=0 - Međunarodnu policijsku organizaciju za kriminal – INTERPOL (pregledano: 04.03.2012.)

[10] Strategija razvoja Agencije za identifikacijska dokumenta, evidenciju i razmjenu podataka Bosne i Hercegovine za period 2010 – 2015, usvojena na 120. sjednici Vijeća ministara 29. 04. 2010. godine.

[11] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42771 - (pregledano: 04.03.2012.)

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:HTML - No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (pregledano: 02.03.2012.)

[13] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF(pregledano: 05.03.2012.)

[14] http://www.nxp.com/(pregledano: 06.03.2012.)

[15] http://www.icao.int/publications/Documents/9303_p1_v2_cons_en.pdf (pregledano: 04.03.2012.)

[16] http://www.iddeea.gov.ba/index.php?option=com_content&view=article&id=161&Itemid=60&lang=hr- Pravilnik o sadrzaju elektoničkog memorijskog elementa putnih isprava BiH(pregledano: 07.03.2012.)

[17] https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html - Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC) (pregledano: 07.03.2012.)

[18] S. Nogo, S. Macan, "E-usluge", SMART E-GOVERNMENT konferencija, Beograd, 2009.

[19] Završni izvještaj, Projekat: Uvezivanje opština u procesu implementacije projekta za biometrijske putne isprave – elektronski pasoš. IDDEEA-SIDA-Švedska, 2009.

ABSTRACT

Upon introduction of minimum security standards for travel documents and passports for the Member States in 2000, European Union has upgraded, standardized and harmonized minimum security requirements and included biometrical requirements for passports and travel documents and made them obligatory for BiH when it comes to this field and establishment of the visa free regime for BiH citizens. Minimum security standards for travel documents and passports of the states cover the use of specific materials, machine readable page containing biographic data, printing techniques, copy protection, techniques for issuance. Pursuant to EU standards covering the field of biometric requirements, they shall meet the standards foreseen by the International Civil Aviation Organization – ICAO. This paper will outline general components of the system for usage of biometric data and their mutual exchange between the competent authorities in BiH public administration.

USAGE OF BIOMETRIC DATA AND THEIR MUTUAL EXCHANGE IN ID SYSTEMS OF BIH

Srđan Nogo, Siniša Macan
srdjan.nogo@iddeea.gov.ba , sinisa.macan@iddeea.gov.ba