Mehanički utjecaj na postojanost funkcionalnosti i kvalitete elektroničke putovnice

Stražnicky, Željka

Sveučilište u Zagrebu

GRAFIČKI FAKULTET

Željka Stražnicky

MEHANIČKI UTJECAJ NA POSTOJANOST FUNKCIONALNOSTI I KVALITETE ELEKTRONIČKE PUTOVNICE

MAGISTARSKI RAD

Zagreb, 2011

University of Zagreb

FACULTY OF GRAPHIC ART

Željka Stražnicky

MECHANICAL INFLUENCE ON THE FUNCTIONAL STABILITY AND QUALITY OF ELECTRONIC PASSPORT

MASTER THESIS

Zagreb, 2011

Sveučilište u Zagrebu

GRAFIČKI FAKULTET

Željka Stražnicky

MEHANIČKI UTJECAJ NA POSTOJANOST FUNKCIONALNOSTI I KVALITETE ELEKTRONIČKE PUTOVNICE

MAGISTARSKI RAD

Mentor(i):

Doc.dr.sc. Damir Modrić

Zagreb, 2011

University of Zagreb

FACULTY OF GRAPHIC ART

Željka Stražnicky

MECHANICAL INFLUENCE ON THE FUNCTIONAL STABILITY AND QUALITY OF ELECTRONIC PASSPORT

MASTER THESIS

Supervisor(s):

Doc.d.sc. Damir Modrić

Zagreb, 2011

UDK broj: 655.3.066.36:620:658.5

Povjerenstvo za ocjenu magistarskog rada:

1. prof. dr. sc. Nikola Mrvac, Sveučilište u Zagrebu, Grafički fakultet – predsjednik
2. doc. dr. sc. Damir Modrić, Grafički fakultet u Zagrebu, mentor
3. doc. dr. sc. Mario Barišić, Sveučilište u Osijeku, Filozofski fakultet, vanjski član

Povjerenstvo za obranu magistarskog rada:

1. prof. dr. sc. Nikola Mrvac, Sveučilište u Zagrebu, Grafički fakultet, predsjednik
2. doc. dr. sc. Damir Modrić, Grafički fakultet u Zagrebu, mentor
3. doc. dr. sc. Mario Barišić, Sveučilište u Osijeku, Filozofski fakultet, vanjski član
4. prof. dr. sc. Vesna Džimbeg – Malčić, Sveučilište u Zagrebu, Grafički fakultet, zamjenska članica

Datum obrane magistarskog rada: 4. srpnja 2011. g.

Mjesto obrane magistarskog rada: Sveučilište u Zagrebu, Grafički fakultet

Povjerenstvo za obranu magistarskog rada donijelo je sljedeću odluku:

Obranila – jednoglasnom odlukom Povjerenstva;

Zagreb, 4. srpnja 2011. g.

SADRŽAJ

1. SAŽETAK

Elektronička putovnica, također poznata kao e-putovnica ili biometrijska putovnica, je kombinirani papirnati i elektronički oblik putovnice koji pored uobičajenih podataka o nositelju putovnice sadrži i biometrijske elektroničke podatke za provjeru autentičnosti identiteta putnika. Cilj ovoga rada je utvrditi ovisnost kvalitete i funkcionalnosti (komunikacijsko svojstvo) e-putovnice o vrsti nosećeg medija i poziciji beskontaktnog čipa unutar elektroničke putovnice (e-putovnice) temeljen na testovima izdržljivosti što se očituje u ispravnosti rada čipa putovnice.

Kako bi se utvrdila navedena povezanost, primijenit će se metode testiranja mehaničkog djelovanja na uzorke e-putovnica različitih svjetskih proizvođača polikarbonatnih identifikacijskih stranica i elektroničkih korica, u skladu sa specifikacijama za testiranje izdržljivosti strojno čitljivih putnih isprava međunarodnog standardizacijskog tijela za putne isprave – ICAO (*Durability of machine readable passports, version: 3.2, date: 2006-08-30*).

2. KLJUČNE RIJEČI

e-putovnica, PC identifikacijska stranica, polimerna identifikacijska stranica, e-korice, standardizacija, strojno čitljive putovnice, personalizacija, beskontaktni čip, antena, zaštita, sigurnost, autentifikacija, autentifikacijski mehanizmi, autentičnost, integritet, originalnost, biometrija, otisci prstiju, slika lica, PKI infrastruktura, proizvodni koncept, mehanički utjecaj, izdržljivost, životni vijek, funkcionalnost, interoperabilnost.

3. ABSTRACT

Electronic passport, also known as e-passport or biometric passport is a combined paper and electronic form of passport which besides usual holder data contains also a biometric data for authentication of identity of passengers. The aim of this study was to determine the dependence of the quality and functionality (communication ability) e-passport on the type of carrier medium and the position of contactless chip in the electronic passport based on durability tests which is reflected in the validity of the passport chip.

To determine the association listed, apply the methods of testing mechanical action on the samples e-passport different polycarbonate data pages and electronic covers manufacturers in the world, in accordance with the specifications for the endurance test machine-readable travel documents of international standardization body for travel documents - ICAO (Durability of machine readable passports, version: 3.2, date: 2006-08-30).

4. KEY WORDS

e-passport, PC data page, polymer data page, e-covers, standardisation, machine readable passport, personalization, contactless chip, antenna, protection, security, authentication, integrity, authentication mechanism, authenticity, originality, biometry, fingerprints, face image, PKI infrastructure, production concept, mechanical influence, durability, lifecycle, functionality, interoperability.

5. UVOD

Ovaj rad je koncipiran tako da sadrži teorijski dio koji obrađuje osnovne segmente sustava izdavanja i proizvodnje e-putovnica u skladu sa važećim svjetskim standardima, te eksperimentalni dio koji je koncentriran na istraživanje utjecaja odabranih mehaničkih testova izdržljivosti na kvalitetu i funkcionalnost e-putovnice.

Ideja za navedeno istraživanje potaknuta je praktičnim iskustvima rada i tehničke koordinacije u projektu “*Biometrijska e-putovnica hrvatskih državljana*“ unutar tvrtke Agencija za komercijalnu djelatnost d.o.o. te osobnim afinitetima koji su usmjereni ka novim generacijama visoko zaštićenih grafičkih proizvoda sa elektroničkom funkcionalnošću. Središte istraživanja je putovnica kao najsloženiji visoko zaštićeni grafički proizvod danas, te ujedno najvažniji proizvod tvrtke. Time je zaslužila posebnu pozornost pri istraživanju parametara koji utječu na njenu funkcionalnost i kvalitetu. U fokusu istraživanja nalazila se elektronička komponenta putovnice kao glavno obilježje nove generacije putovnica koje još uvijek nisu doživjele svoju punu zrelost u sustavima proizvodnje i uporabe na tržištu. Zrelost sustava proizvodnje i uporabe e-putovnica na tržištu podrazumijeva iskustvene doživljaje sa „terena“ pri normalnoj uporabi tokom njihovog životnog vijeka od 10 god. Kako su se elektroničke putovnice prvi put počele izdavati 2004. god. (Belgija), najranije 2014. god. moći će se točnije analizirati i sagledati aspekti koji utječu na njenu kvalitetu te donijeti konkretniji zaključci koji će determinirati daljnji smjer razvoja samog dokumenta ali i sustava u cijelosti.

U istraživanju i izradi magistarskog rada korišteni su materijali prikupljeni tokom rada na projektu, informacije stečene vlastitim istraživanjem i poslovnim susretima s velikim svjetskim proizvođačima materijala, poluproizvoda i gotovih proizvoda, strojeva, softvera, više ili manje cjelovitih sustava izdavanja i uporabe, sudjelovanjem na specijalističkim svjetskim konferencijama i radu sa Ministarstvom unutarnjih poslova RH.

Određene informacije i saznanja nisu mogle biti publicirane zbog osjetljivosti materije, uloge AKD-a kao jedinog ovlaštenog proizvođača sigurnosnih dokumenta u Republici Hrvatskoj te poslovne orijentacije ka štićenju i čuvanju poslovnih tajni iz segmenta visoko zaštićenog proizvodnog programa. Unatoč tome, radom su prikazani svi ključni elementi sustava sa svojim funkcionalnim specifikacijama i zakonitostima.

U provedbi testova korištena je oprema za testiranje e-putovnica u vlasništvu AKD-a, nabavljena u sklopu navedenoga projekta za potrebe kontinuiranog i sustavnog praćenja kvalitete proizvodnje putovnica. Ispitivana su 4 tipa putovnica različitih svjetskih proizvođača e-korica i polikarbonatnih (u daljnjem tekstu PC) identifikacijskih stranica s naglaskom na specifičnost medija koji pohranjuje elektroničku „pamet“ putovnice. Količina prikupljenih e-korica i PC identifikacijskih stranica odredila je mogućnost primjene broja metoda testiranja. Prikupljeni uzorci e-korica i PC identifikacijskih stranica morali su sadržavati potpuno funkcionalni, tzv. „živući“ čip koji je bio glavni pokazatelj utjecaja primijenjenih metoda na funkcionalnost i kvalitetu putovnice.

Dobiveni rezultati testiranja, kao i prikupljene informacije o materiji izrade e-putovnica, činili su temelj za donošenje zaključka o optimalnom smještaju čipa u putovnici, te odabranom proizvodnom konceptu izrade i personalizacije.

6. POVJEST RAZVOJA PUTOVNICE

Jedan od najranijih dokaza postojanja putovnice je zabilježen u Hebrejskoj Bibliji. U dijelu Biblije koji govori o Nehemiah-u (2:7-9) u vremenu Perzijskog Carstva, 450. g.pr.k., Nehemiah je zatražio tadašnjeg kralja Perzijskog Carstva Artaxerxes I. dozvolu putovanja u Judeju.
Kao dozvolu putovanja Nehemiah je dobio od kralja pismo koje je upućeno „državnim upraviteljima-guvernerima iza rijeke“ u kojem ih moli za siguran prolaz putnika kroz njihove zemlje. U nekim današnjim putovnicama, kao npr. kanadskoj, ovakvo pismo stoji na unutrašnjoj strani korica putovnice te je objavljeno u ime njezinog veličanstva kraljice. Kraljica, na simboličan način, traži zaštitu putnika i sigurni prolaz kroz razna teritorija.

U srednjovjekovnoj Europi putni dokumenti izdavali su se putnicima od strane lokalnih vlasti, a sadržavali su listu gradova u koje je putnik smio ući. Takvi dokumenti nisu bili zahtijevani za uplovljavanje u luke, koje su se smatrale otvorenim trgovačkim središtima, već za ulazak iz luke u unutrašnjost zemlje.

U srednjovjekovnom islamskom Kalifatu putovnica se izdavala u obliku potvrde o plaćenim porezima, a zvala se *bara´a*. Samo oni građani koji su plaćali obavezne poreze imali su pravo putovati unutar područja Kalifata.

Francuski kralj Louis XIV. je u vrijeme svoje vladavine (1638. – 1715.) izdavao pisma potvrde koje je osobno potpisivao svojim dvorskim službenicima. Takvo pismo nazivalo se „*passe port*“, što bi značilo - *onaj koji prolazi kroz luku ili gradska vrata* -, jer se u većini međunarodnih putovanja koristio brod kao prijevozno sredstvo. Otuda je nastao naziv *passport* ili putovnica.
U vrijeme vladavine Louis-a XIV. gotovo svaka europska država je uspostavila svoj sustav izdavanja putovnica. Osim što su morali imati putovnice svojih matičnih država, putnici su trebali imati i vize izdane od strane država koje su željeli posjetiti, slično kao što je to i danas.

Slika 1 – kineska putovnica iz dinastije Qing, 1898.god. (desno), engleska putovnica (leighton) iz 1883.god. (lijevo)

Izradila: Željka Stražnicky, lipanj 2011.

Slika 2 – prva japanska putovnica izdana 1866.god. (desno), crnogorska putovnica iz 1887.god. (lijevo)

Sredinom 19. stoljeća velika ekspanzija putovanja željeznicom je uslijed povećanog turizma dovela do potpunog pada sustava izdavanja i korištenja putovnica. Zbog brzine vlakova, količine vlakova i putnika, zakoni koji propisuju uporabu putovnice nisu bili održivi. Zbog navedene krize prva je Francuska ukinula putovnice i vize 1861.god., a zatim su i sve ostale europske države slijedile njezin primjer. Do 1914. god. putovnice i vize više nisu bile u uporabi.

Prvi svjetski rat ponovno je obnovio zabrinutost vezanu uz međunarodnu sigurnost, te su putovnice i vize opet bile zahtijevane, doduše kao privremena mjera. Obnovljene mjere kontrole zadržane su ipak i poslije rata, a postale su i standardna procedura. Tada su se prvi puta pojavile i sumnje vezane uz zaštitu privatnosti, naročito zbog priloženih fotografija i fizičkog opisa u putovnicama, koje su prema riječima britanskih turista vodile do podmukle dehumanizacije.

Niz međunarodnih konferencija o putovnicama (1920., 1926. i 1947.) pod nazivom „*International Conference on Passports, Customs Formalities and Through Tickets“* dovele su do novih specifikacija putovnica. Konferencija održana 1920. god. donijela je slijedeće preporuke: putovnica je trebala biti izrađena u obliku knjižice formata 15,5 x 10,5 cm sa jedinstvenim stilom izrađenim prema identičnom standardu, tekst unutar putovnica trebao je biti tiskan na najmanje 2 jezika, od kojih je jedan francuski, a drugi nacionalni jezik, 32 stranice putovnice sve numerirane i uvezane u korice na bazi kartona te preporučena valjanost putovnice od najmanje 2 god., a poželjno 5 god. Potpuno nove redizajnirane putovnice trebale su zamijeniti stare do srpnja 1921. god. 1926. i 1927. god. izašle su smjernice za izradu dizajna knjižica putovnice.

Izradila: Željka Stražnicky, lipanj 2011.

7. ICAO STANDARDIZACIJA

Veći napredak u standardizaciji putovnica bio je evidentniji nakon 2. Svjetskog rata, s kulminacijom ratifikacije konvencije u Chicago-u 1947. god. U sklopu ove konvencije, sve države članice novo oformljene organizacije ICAO (*International Civil Aviation Organization*) složile su se oko usvajanja novih mjera koje se tiču zračnog prometa. ICAO je postavio nove standarde i odredbe neophodne za zračnu sigurnost, učinkovitost, redovitost i zaštitu okoliša u sklopu zrakoplovne industrije. Novi standard bio je pokriven sa ukupno 18 aneksa, od kojih su za putne dokumente bili značajni aneksi koji govore o sigurnosti i pojednostavljenju kontrole.

Unatoč ovim nastojanjima standardizacije, dokumenti putnih isprava bili su i dalje niske tehnološke razine (papiri niske kvalitete bez implementiranih zaštitnih elemenata i sa fotografijom nositelja putovnice).

Ujedinjeni narodi održali su konferenciju o putnim dokumentima 1963. god., no ona nije rezultirala novim smjernicama za izradu putovnica.

Tek je 1980. god. pod okriljem organizacije ICAO proizašla prava standardizacija putovnica. Tada se dogodio i prvi veliki tehnološki napredak u obliku strojno čitljivih putovnica (*Machine Readable Passports – MRP*) predstavljenih u SAD-u 1981. god. u sklopu prvog izdanja danas vrlo korištenog dokumenta ICAO Doc 9303. Pojava strojno čitljivih putovnica primarno je bila poticana velikim porastom zračnog prometa te potrebom automatizacije kontrola putovnica na graničnim prijelazima radi veće brzine protoka putnika te sigurnosti. Nekoliko europskih država primijenilo je standard u slijedećim godinama.

Učinkovitost ICAO organizacije ležala je u kooperaciji sa specijaliziranim agencijama UN-a, suradnji s državama članicama i drugim standardizacijskim tijelima poput ISO (*International Organization for Standardization*). Radna grupa ISO organizacije razvila je dodatne specifikacije koje su prihvaćene 1985. god. u obliku dokumenta ISO 7501 (*Identification cards – Machine Readable Passports*).

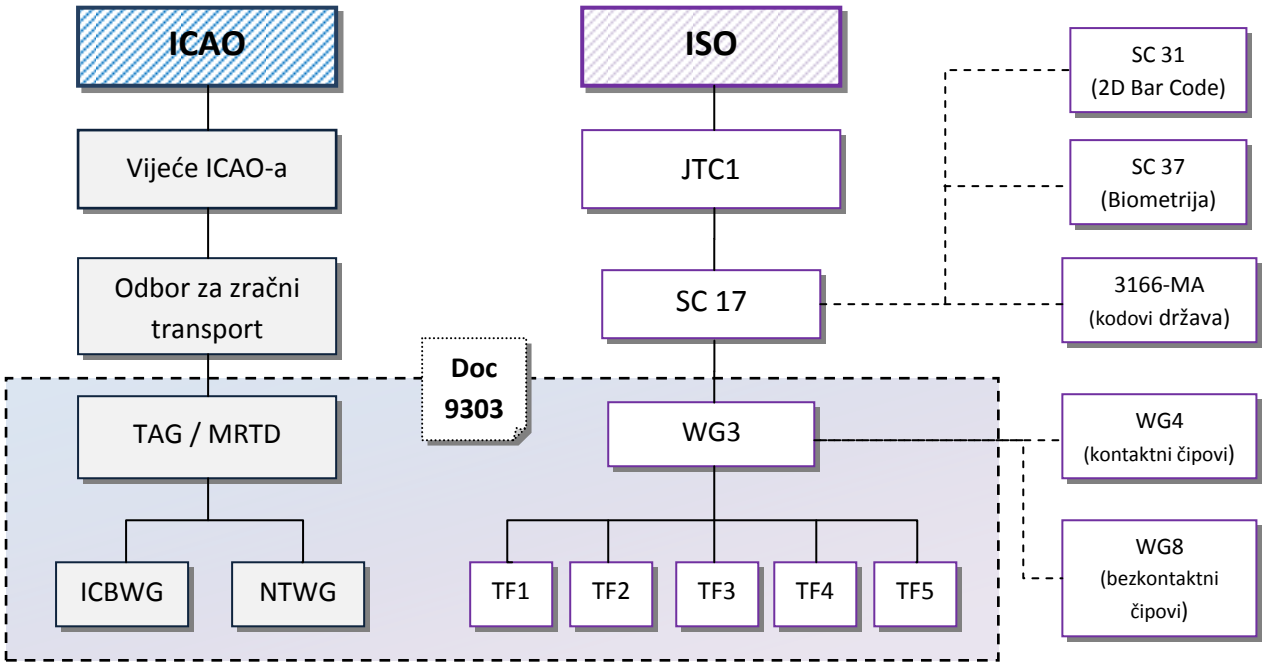
1984. god. osnovana je tehničko savjetodavna grupa (*TAG – Technical Advisory Group*) za strojno čitljive putovnice pri ICAO-u koja je imala savjetodavnu ulogu kao i ulogu preispitivanja i nadogradnje specifikacija vezanih uz putne isprave povezanih s praktičnim iskustvima sa terena. Nedugo nakon toga ICAO je odlučio preuzeti vodstvo u razvoju specifikacija putnih isprava kako bi osigurao jedinstveni set standarda. Tada je prvi put prepoznata potreba da se u specifikacije ugrade i tehničke preporuke za dobavljače repromaterijala i proizvođače putovnica.

Suradnja ICAO i ISO organizacije je i dalje nastavljena, te je ISO nastavio rad na unaprjeđenju standarda ISO 7501, kao potporu dokumentu ICAO Doc 9303. Nastali su novi nastavci dokumenta, ISO 7501-1, ISO 7501-2 i ISO 7501-3.

I druge organizacije su surađivale s ICAO organizacijom, a među njima su: Međunarodno vijeće zračnih luka (*Airport Council International – ACI*), Međunarodna asocijacija o zračnom prometu (*International Air Transport Association – IATA*), Međunarodna organizacija kriminalističke policije (*International Criminal Police Organization – INTERPOL*) i Europska komisija (*European Comission – EC*).

Već spomenuta ICAO TAG MRTD grupa sastoji se od stručnjaka predstavnika država članica ICAO-a iz različitih organizacija i industrije. Njihov cilj je kontinuirano unaprjeđivati zaštitu i učinkovitost strojno čitljivih putovnica. No, kako se povećavala kompleksnost i volumen posla, morale su se osnovati dodatne specijalističke radne grupe.

Tako je nastala radna grupa za nove tehnologije (*New Technologies Working Group – NTWG*) sa ciljem istraživanja tehnologija izrade putnih dokumenata, analize i razvoja strategija, politika i novih dodataka dokumentu 9303 Doc. Radna grupa također izrađuje i smjernice koje objašnjavaju i podupiru standardizaciju i interoperabilnost putnih dokumenata te tehničke izvještaje koji sadrže nacrte novih specifikacija za što brže informiranje interesnih skupina. Ova grupa blisko surađuje sa radnom grupom ISO organizacije, a njihovo partnerstvo kao i organizacija prikazane su na slici 3 [3].



**JTC1 – Joint Commitee 1 (udruženi odbor)*
SC 17 – Sub-Commitee 17 (Pod-odbor br.17 zadužen za kartice i osobnu identifikaciju)
WG 3 – Working Group 3 (Radna grupa zadužena za MRTD
TAG – Technical Advisory Gorup
MRTD – Machine Readable Travel Documents
ICBWG- Implementation and Capacity Building Working Group
NTWG – New Technology Working Group

Slika 3 - Organizacijska struktura ICAO-a i ISO-a te korelacija

Izradila: Željka Stražnicky, lipanj 2011.

7.1. Prekretnica u ICAO specifikacijama [6]

Početkom 1996. god. ICAO je prvi put razmatrala unaprjeđenje sigurnosti strojno čitljivih putnih dokumenata. U to doba se također uzela u obzir i mogućnost implementacije biometrijskih značajki u dokument, te standardizacija na području identifikacijskih sustava općenito.

Razmatrajući nekoliko tehnologija kao što su 2D i 3D barkod, organizacija je naposljetku odluku donijela u korist implementacije beskontaktnog integriranog kruga (beskontaktnog čipa) u strukturu dokumenta te uporabe biometrijske identifikacije 2000. god.

Iako su događaji od 11. rujna 2001. god. ponešto ubrzali proces predstavljanja novih sigurnosnih elemenata putovnice, ICAO je već bio ostvario popriličan napredak ka definiranju novih specifikacija putovnice te ih predstavio iste 2001. god. Nove specifikacije označavale su tzv. **elektroničku putovnicu 1. generacije (e-putovnica)**. Osnovna značajka 1. generacije e-putovnica bila je uvođenje slike lica kao primarnog biometrijskog identifikatora u strukturu beskontaktnog čipa.

Kao reakciju na događaj od 11. rujna 2001. god., SAD je zatražila od članica *Visa Waiver* programa (članice ovog programa oslobođene su potrebe izdavanja Viza za ulazak u SAD) izdavanje e-putovnica 1. generacije do 26. listopada 2004. god.; u protivnom bi za ulazak njihovih građana u SAD bile ponovno zahtijevane vize. Također, budući da su još uvijek postojale države svijeta koje nemaju niti strojno čitljive putovnice (kao i danas) navela je da je za ulazak u SAD nužno posjedovanje strojno čitljive putovnice u protivnom ulazak u SAD neće biti moguć.
Budući da su nove specifikacije zahtijevale brzi odziv tržišta te ponudu kvalitetnih i sigurnih rješenja, čekanje odgovarajućeg tehnološkog razvoja je dvaput prolongiralo rok koji je u konačnici bio definiran na 26.10.2006. god.

Gotovo sve članice *Visa Waiver* programa uspjele su izaći u susret postavljenom roku te izdale svoje e-putovnice 1. generacije. Među prvima je bila Belgija koja je izdala e-putovnicu 1.generacije već u studenom 2004. god.

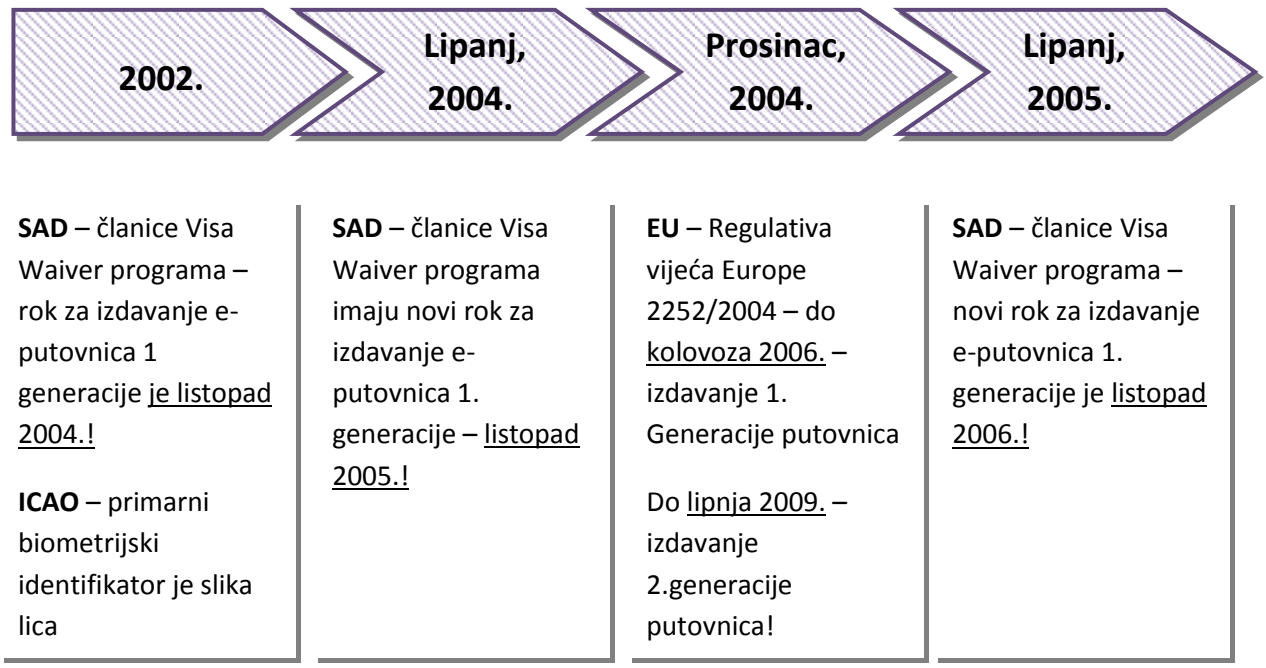
2004. god. Europska Unija je odlučila podići ljestvicu složenosti i zaštite e-putovnica te je pored osnovnih ICAO specifikacija zahtijevala i uporabu otisaka prstiju kao obaveznog i sekundarnog biometrijskog identifikatora u e-putovnicama za svoje članice. Budući da se otisci prstiju smatraju naročito osjetljivim podacima koji u slučaju krađe mogu otvoriti vrata dodatnoj mogućnosti, teško osporivog, lažnog predstavljanja, sigurnosni elektronički mehanizmi čipa morali su biti unaprijeđeni u odnosu na one 1. generacije e-putovnica. Tako je za novu generaciju e-putovnica zahtijevano slijedeće: ispunjenje sigurnosnih zahtjeva 1. generacije, implementacija dva otiska prsta, implementacija dodatnih sigurnosnih autentifikacijskih mehanizama tzv. proširene kontrole pristupa (*Extended access control - EAC*). Ova nova generacija putovnica označava **elektroničke putovnice 2. generacije**.

Europska Unija je tako za implementaciju 2. generacije e-putovnica svojim članicama postavila rok, lipanj, 2009. god. (rok koji je također prolongiran za godinu dana u odnosu na prvotno postavljeni).

No kako je ICAO u svojem standardu definirao samo mehanizme zaštite 1. generacije e-putovnica, za e-putovnice 2. generacije tek je bilo potrebno definirati i objaviti autentifikacijske mehanizme koji bi štitili otiske prstiju od neautoriziranog pristupa.

ICAO je prihvatio i preporučio proširenu kontrolu pristupa, specifikacije koje je razvila BIG organizacija (*Brussels Interoperability Group*) unutar Europske Unije. Veliki obol definiranju ovog standarda dalo je i njemačko standardizacijsko tijelo – BSI (*Bundesamt fűr Sicherheit in der Informationstechnik*), pa činjenica da je upravo Njemačka prva izdala e-putovnicu 2. generacije (studeni, 2007.) nimalo ne iznenađuje.

Posljednji službeni podatak objavljen u stručnom časopisu Keesing [5] kaže da je do danas 46 država svijeta izdalo putovnice 2. generacije za sve vrste svojih putovnica, 5 država je specifikacije ugradilo samo u jednu ili dvije vrste svojih putovnica (diplomatska ili službena putovnica) i 1 država koja je ugradila vlastite specifikacije u 2. generaciju drugačije od onih propisanih od strane EU. Većina navedenih država (31) su europske države, no iako je mandat za uvođenje putovnice 2. generacije vrijedio isključivo za Europsku Uniju, specifikacije su prihvaćene kao međunarodni standard.



Slika 4 –Vremenska skala najvažnijih događaja

7.2. ICAO dokumentacija

ICAO specifikacije su se tijekom godinama proširile tako da obuhvaćaju ne samo specifikacije strojno čitljivih putovnica već i specifikacije svih ostalih vrsti strojno čitljivih putnih dokumenata.
Doc 9303 sastoji se od 3 osnovna dijela: 1. dio koji obuhvaća specifikacije za putovnice, 2. dio koji obuhvaća specifikacije za vize i 3. dio koji obuhvaća ostale službene identifikacijske dokumente. Pojedini dijelovi imaju svoje sveske koji se bave određenim specifičnostima [4].

Naziv dokumenta	Izdanje	Godina
Part 1 - Machine Readable Passport - Volume 1 *Passports with Machine Readable Data Stored in Optical Character Recognition Format* – (1. Dio – Strojno čitljive putovnice – Svezak 1 - Putovnice sa strojno čitljivim podacima pohranjenima u formatu optički prepoznatljivih znakova).	6. izdanje	2006.
Part 1 - Machine Readable Passport - ***Volume 2*** *Specifications for Electronically Enabled Passports with Biometric Identification Capabilities* – (1. Dio – Strojno čitljive putovnice – Svezak 2 - Specifikacije za elektroničke putovnice sa mogućnošću biometrijske identifikacije).	6. izdanje	2006.
Part 2 - Machine Readable Visas – (2. Dio – Strojno čitljive vize)	3. izdanje	2005.
Part 3 - ***Machine Readable Official Travel Documents - Volume 1*** *MRtds with Machine Readable Data Stored in Optical Character Recognition Format* – (3. Dio Strojno čitljivi službeni putni dokumenti – Svezak 1 – Putni dokumenti sa strojno čitljivim podacima pohranjenima u formatu optički prepoznatljivih znakova).	3. izdanje	2008.
Part 3 - ***Machine Readable Official Travel Documents - Volume 2*** *Specifications for Electronically Enabled MRtds with Biometric Identification Capability* – (3. Dio – Strojno čitljive putni dokumenti – Svezak 2 - Specifikacije za elektroničke putovnice sa mogućnošću biometrijske identifikacije).	3. izdanje	2008.

Tablica 1 – Popis aktualnih ICAO dokumenata vezanih uz strojno čitljive putne isprave

Povremeno se izdaju i dodaci dokumentu Doc 9303 (*Suplements & Technical Reports*) u obliku tehničkih izvještaja, koji služe dodatnim pojašnjenjima, a sadrže i ispravke uzrokovane implementacijskim iskustvima.

8. SPECIFIKACIJE STROJNO ČITLJIVIH PUTOVNICA

Kako bi se podigla razina zaštite putnog dokumenta te smanjile prijetnje od krivotvorenja, tijekom godina je razvijeno niz metoda i tehnologija za izradu repromaterijala te tehnika za personalizaciju (dodavanje varijabilnih podataka na dokument). Iako neki od zaštitnih elemenata mogu pružiti istu zaštitu od određene prijetnje (npr. zamjena slike, odstranjivanje stranica KB-a, izmjena strojno čitljive zone i sl.), još uvijek ne postoji jedan zaštitni element koji bi pružio 100%-tnu zaštitu od svih vrsti prijetnji. Zbog toga se u praksi primjenjuje kombinacija različitih zaštitnih elemenata kako bi s postigla najbolja ravnoteža za obranu od krivotvorenja.

Specifikacije za izradu strojno čitljivih putovnica mogu se podijeliti u nekoliko osnovnih grupa:

- Repromaterijali (Knjižni blok (KB), Predlist/zalist (P/Z), Konac za šivanje, Korice)
- Sigurnosni tisak (Podloga, Stranica sa podacima, Boje, Numeracija)
- Zaštita od kopiranja
- Personalizacijske tehnike

REPROMATERIJALI – KNJIŽNI BLOK

zahtjev	Ref. standard	obavezni / opcionalni
Otpornost prema refleksiji UV izvora zračenja	[7]	*obavezni*
Vodeni znak – dvotonski ili višetonski	[7]	*obavezni*
Papir odgovarajuće apsorpcije i hrapavosti	[7]	*obavezni*
Kemijska osjetljivost papira – kemijski markeri	[7]	*obavezni*
Vodeni znak u registru	[7]	*opcionalni*
Nevidljiva luminiscentna vlakna i/ili planšete	[7]	*opcionalni*
Vidljiva luminiscentna vlakna i/ili planšete	[7]	*opcionalni*
Sigurnosna nit u masi papira ili „window“nit	[7]	*opcionalni*

Tablica 2 – Popis preporuke zaštitnih elemenata knjižnog bloka strojno čitljivih dokumenata

REPROMATERIJALI – PREDLIST/ZALIST (P/Z)

zahtjev	Ref. standard	obavezni / opcionalni
Kemijska osjetljivost papira – kemijski markeri	[7]	*obavezni*
Zbog toga što P/Z ne mora imati vodeni znak, odgovarajuća zaštitna metoda mora biti primijenjena kako bi se postigao visoki stupanj zaštite ukoliko se P/Z koristi kao stranica sa podacima nositelja putovnice	[7]	*obavezni*

Tablica 3 – Popis preporuke zaštitnih elemenata predlista/zalista strojno čitljivih dokumenata

REPROMATERIJALI – KONAC ZA ŠIVANJE

zahtjev	Ref. standard	obavezni / opcionalni
Šivanje sa uporabom pozadinskog konca za ojačanje uveza	[7]	*obavezni*
Stranica sa podacima kao integrirani dio (ušiveni) sa svojim sigurnosnim laminatom u KB	[7]	*opcionalni*
Višebojni i/ili luminiscentni konac za šivanje	[7]	*opcionalni*
Podesivi uzorak šivanja	[7]	*opcionalni*

Tablica 4 – Popis preporuke zaštitnih elemenata vezanih uz konac za šivanje strojno čitljivih dokumenata

REPROMATERIJALI – KORICE

zahtjev	Ref. standard	obavezni / opcionalni
Boja platna – burgundy crvena što bliža RAL 4004 standardu	[33]	*obavezni*
Informacije na platnu, ime države, grb države, naziv dokumenta	[33]	*obavezni*

Tablica 5 – Popis preporuke zaštitnih elemenata korica strojno čitljivih dokumenata

SIGURNOSNI TISAK – PODLOGA

zahtjev	Ref. standard	obavezni / opcionalni
Dvobojni guilloche	[7]	*obavezni*
Iris tisak	[7]	*obavezni*
Antikopirajući uzorci	[7]	*obavezni*
Mikrotisak	[7]	*obavezni*
Dizajn podloge strancie sa podacima nositelja putovnice mora biti drugačiji od dizajna stranica KB-a	[7]	*obavezni*
Intaglio tisak – jednobojni ili višebojni – na predlistu, zalistu ili na stranicama KB-a, ili na oba	[7]	*opcionalni*
Latentna slika u Intaglio tehnici	[7]	*opcionalni*
Izdignuti (3D) element	[7]	*opcionalni*
„Prozirni“ registar	[7]	*opcionalni*
Namjerna greška u mikrotisku	[7]	*opcionalni*

Tablica 6 – Popis preporuke zaštitnih elemenata sigurnosnog tiska strojno čitljivih dokumenata

SIGURNOSNI TISAK – STRANICA SA PODACIMA

zahtjev	Ref. standard	obavezni / opcionalni
Integracija slike nositelja u podlogu	[7]	*obavezni*
Sigurnosni tisak (*guilloche*) prelazi preko područja slike	[7]	*obavezni*
Laminat ili overlay na bazi vruće laminacije preko slike	[7]	*obavezni*
Optički varijabilni element (hologram) položen na sliku	[7]	*opcionalni*
Integrirane steganografske (sakrivene) slike	[7]	*opcionalni*
Dodatna slika nositelja	[7]	*opcionalni*
Pohrana i mogućnost povrata digitalne slike u sustavu	[7]	*opcionalni*
Biometrijski element	[7]	*opcionalni*

Tablica 7 – Popis preporuke zaštitnih elemenata stranice sa podacima strojno čitljivih dokumenata

SIGURNOSNI TISAK - BOJE

zahtjev	Ref. standard	obavezni / opcionalni
UV luminiscentna boja (vidljiva ili nevidljiva) na stranici sa podacima nositelja i na svim stranicama KB-a	[7]	*obavezni*
Kemijski reaktivne boje, tamo gdje je podloga papir ili barem na stranici sa podacima nositelja	[7]	*obavezni*
Boje sa optički varijabilni svojstvima – OVI boje	[7]	*opcionalni*
Boje na bazi metala	[7]	*opcionalni*
Penetrirajuće boje za numeriranje	[7]	*opcionalni*
Metameričke boje	[7]	*opcionalni*
Infracrvene boje (koje nestaju u IR spektru)	[7]	*opcionalni*
Termokromatske boje	[7]	*opcionalni*
Fotokromatske boje	[7]	*opcionalni*
IR luminiscentne boje	[7]	*opcionalni*
Fosforescentne boje	[7]	*opcionalni*
Boje sa mikro/nano tagantima	[7]	*opcionalni*

Tablica 8 – Popis preporuke zaštitnih elemenata tiskarskih boja strojno čitljivih dokumenata

SIGURNOSNI TISAK – NUMERACIJA

zahtjev	Ref. standard	obavezni / opcionalni
Jedinstveni broj putovnice mora se pojavljivati na svim stranicama putovnice izuzev na P/Z-u	[7]	*obavezni*
Broj putovnice će biti ili otisnut ili perforiran, Ukoliko je tiskan mora biti otisnut strojno čitljivim fontom te vidljivom UV luminiscentnom bojom	[7]	*obavezni*

Tablica 9 – Popis preporuke zaštitnih elemenata vezanih uz numeraciju strojno čitljivih dokumenata

ZAŠTITA OD KOPIRANJA

zahtjev	Ref. standard	obavezni / opcionalni
Optički varijabilni element (hologram) mora biti upotrijebljen barem na stranici sa podacima nositelja	[7]	*obavezni*
Optički varijabilni element mora se nalaziti u strukturi stranice sa podacima nositelja	[7]	*obavezni*

Tablica 10 – Popis preporuke zaštitnih elemenata vezanih uz zaštitu od kopiranja strojno čitljivih dokumenata

PERSONALIZACIJSKE TEHNIKE

zahtjev	Ref. standard	obavezni / opcionalni
Elektro-fotografski tisak	[7]	*opcionalni*
Termal transfer tisak	[7]	*opcionalni*
Ink jet tisak	[7]	*opcionalni*
Fotografski procesi	[7]	*opcionalni*
Lasersko graviranje	[7]	*opcionalni*

Tablica 11 – Popis preporuke zaštitnih elemenata vezanih uz personalizacijske tehnike

Izradila: Željka Stražnicky, lipanj 2011.

8.1. Zaštitni elementi putovnica

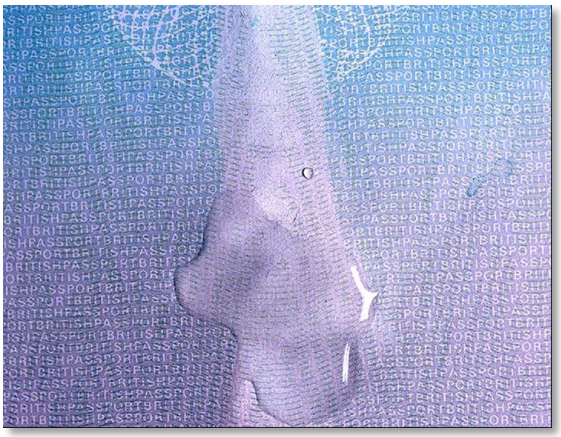
UV fluorescencija / luminiscencija

Svojstvo boje, pri normalnom osvjetljenju vidljive ili nevidljive, da luminiscira, odnosno reflektira određenom valnom duljinom vidljivog spektra zračenja pri izlaganju UV spektra zračenja određene valne duljine. UV boje mogu biti otisnute različitim tehnikama tiska, a u izradi dokumenata, najčešće se otiskuju tehnikama ofseta i sitotiska.

Slika 5 - UV luminiscirajući tisak u knjižnom bloku RH, UV luminiscirajuća traka za šivanje, metalna nit te vlakanca koja su sastavni dio papira (izvor: AKD)

Osjetljivost na otapala

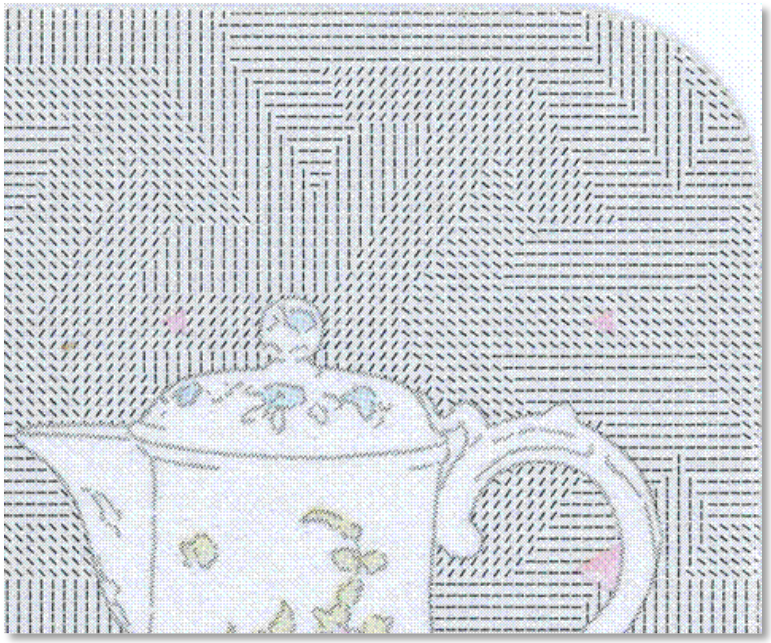
Jedno od svojstava zaštitne boje da reagira u kontaktu s otapalima koja se najčešće koriste pri pokušajima krivotvorenja ostavljajući vidljiv trag o pokušaju krivotvorenja.



Slika 6 – Primjer degradacije zaštitne boje kada ju se izloži otapalima

Anti-kopirni uzorak

Sigurnosni element otisnut u pozadinskom području dizajna, a krosti se kao zaštita pri pokušajima reprodukcije putem kopiranja ili skeniranja. Unutar dizajna integriran je sakriveni element, nevidljiv golom oku, koji postaje vidljiv nakon kopiji izrađenoj fotokopiranjem ili skeniranjem.



Slika 7 – Antikopirajući uzorak

OVI boja

OVI (eng. *optical variable ink*) predstavlja optički varijabilnu tiskovnu boju koja daje različiti dojam obojenja kad ju se promatra pri različitim kutovima. Ova boja osim svog zaštitnog svojstva, koje se očituje i u činjenici da nije komercijalno dostupna na tržištu (tj. dostupna je samo ovlaštenim zaštićenim tiskarima), ostavlja i vrlo zanimljiv vizualni dojam.

Slika 8 - OVI uzorak

IR boja

IR (eng. *infrared*) boje pružaju najbolju zaštitu od krivotvorenja među sigurnosnim tiskarskim bojama. One se odlikuju različitom kombinacijom svojstava, pa tako postoje IR boje koje su vidljive pri dnevnom svjetlu, ali pod IR osvjetljenjem postaju nevidljive, zatim IR boje koje su nevidljive pri dnevnom svjetlu, a postaju vidljive u određenom dijelu infracrvenog spektra i dr. Navedena svojstva IR boja pružaju mogućnost otiskivanja skrivenih informacija koje su poznate jedino proizvođaču kartice, pa na taj način predstavljaju odličan element zaštite.
Osim navedenih svojstava, IR boje također mogu i luminiscirati u određenom dijelu spektra UV elektromagnetskog zračenja.

Irisni tisak

Specifična tehnika tiska kojom se pomoću jedne tiskovne forme ostvaruje prava višebojna, višetonska reprodukcija koju je nemoguće krivotvoriti fotokopirnim uređajem, skenerom, klasičnim četverobojnim offsetnim tiskom ili drugim tehnikama tiska.
Zbog svoje specifične zaštite irisni tisak predstavlja standard u tisku visoko-zaštićenih tiskovina poput viza, novčanica, putovnica i dr.

Slika 9 – Irisni tisak (prijelaz iz crvene u plavu) na predlistu putne isprave RH (izvor: AKD)

Intaglio

Specifična, rijetka i vrlo skupa tehnika tiska upotrebljava se isključivo za tisak vrijednosnica poput novčanica i dionica, te putnih dokumenata poput putovnica i viza. Intaglio spada u direktnu tehniku dubokog tiska kod koje se iz tiskovne forme pod vrlo velikim pritiskom boja prenosi na tiskovnu podlogu formirajući opipljivi trodimenzionalni trag kojeg je, upravo zbog opipljive trodimenzionalnosti, nemoguće reproducirati konvencionalnim, jeftinim tehnikama tiska. U kombinaciji sa tehnikom intaglio tisak moguće je kombinirati i tehniku iris tiska čime se dobiva zaštitni element višeg ranga.

Slika 10 - Primjer dvobojnog intaglio tiska (izvor: AKD)

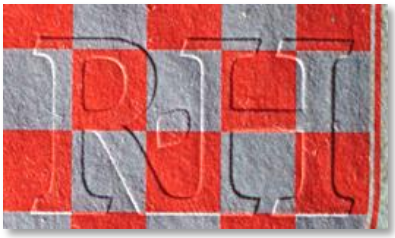
Slika 11 - Primjer trobojnog intaglio_iris tiska

Zbog naglašene trodimenzionalnosti, intaglio tehnikom tiska otiskuje se i zaštitni element latentne slike. Gledajući okomito, tekst/motiv latentne slike nije vidljiv. Zakretanjem putne isprave za cca. 80° latentna slika postaje vidljiva.

Slika 12 - Primjer latentne slike zalista putne isprave RH otisnute intaglio tehnikom tiska (izvor: AKD)

Slijepi tisak

Visoka tehnika tiska koja ne upotrebljava tiskarsku boju već pritiskom deformira tiskovnu podlogu stvarajući opipljivi trodimenzionalni efekt.



Slika 13 - Motiv otisnut slijepim tiskom na predlistu putne isprave RH (izvor: AKD)

Numeracija knjigotiskarskom tehnikom tiska

Knjigotiskarskim numeratotom otiskuje se serijski broj putovnice na predlistu i zalistu sa specifičnom bojom za numeraciju koja ima svojstvo luminiscencije kada se izloži UV izvoru

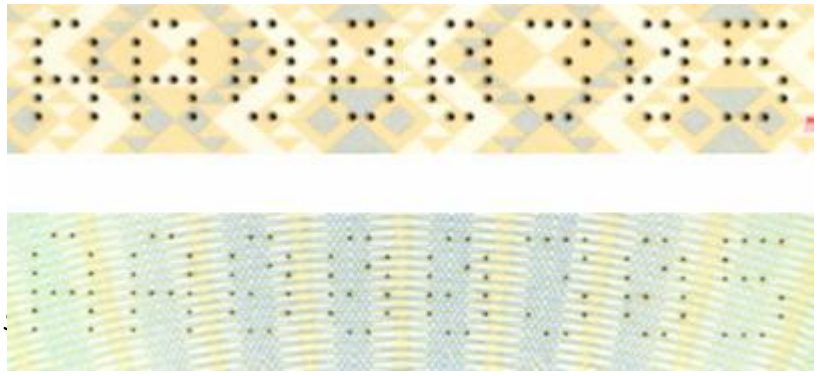
svjetla. Tip znamenki knjigotiskarskog numeratora (font) je specifičan na način da se razlikuje od standardnih fontova numeratora poput OCR A i B fontova. Serijski broj putovnice otisnut na predlistu i zalistu putovnice odgovara serijskom broju na stranici nositelja putovnice i laserski perforiranom serijskom broju na knjižnom bloku i zadnjoj korici putovnica.

Slika 14 - Primjer UV luminiscirajuće knjigotiskarske boje pod UV izvorom svjetla otisnute mehaničkim numeratorom

Laserska numeracija

Svaka proizvedena putna isprava podvrgava se numeraciji specifičnim laserom koji prolaskom kroz knjižni blok putne isprave (izuzev prve strane korica i identifikacijske stranice) nepovratno pali stranice knjižnog bloka i zadnju stranicu korica jedinstvenim deveteroznamenkastim brojem putne isprave.

Uslijed prolaska laserske zrake kroz papir knjižnog bloka dolazi do postepenog gubitka energije paljenja što rezultira zaštitnim elementom koji se očituje u smanjenju promjera propaljene točkice proporcionalno s paginacijski gledano većom stranicom (32. stranica ima manji promjer točkice od 3. stranice knjižnog bloka putne isprave).



Slika 15 – Prva i zadnja stranica sa laserski perforiranom numeracijom

Kinegram®

Kinegram® je visoko-zaštićeni sigurnosni element, brend jedne vrste holograma tvrtke OVD Kinegram AG. Ovaj zaštitni element primarno se koristi za zaštitu državnih dokumenata.
Kako samo ime nalaže, slika Kinegrama® predstavlja kinetičko – optičke efekte koje promatrač može vrlo lako uočiti.

Kinegram® se bazira na jedinstvenom procesu izrade optički varijabilnih linija vrlo visoke rezolucije. Linije su kreirane na način da tvore niz dinamičkih slika koje zakretanjem kinegrama® stvaraju pokret. Svaki kinegram® je izrađen prema zahtjevima kupca, a sastoji se od niza elemenata različitih nivoa sigurnosti.

Neki od tih elemenata su kinetički *guilloche*-i, razne linijske strukture čije kretanje unutar samog kinegrama® može biti linearno, radijalno, rotirajuće, zatim razne mikro-strukture koje ne mogu biti kopirane ni sofisticiranim optičkim tehnikama bez gubitka njihovih karakteristika, nevidljivi mikroprofili koji vrše difrakciju upadnog svjetla i mnogi drugi.

Prednosti Kinegrama® pred standardnim hologramom su slijedeće:

- lagana verifikacija i prepoznatljivost
- velika uočljivost, čak i pri malom osvjetljenju
- kinetička slika
- neograničene mogućnosti izrade dizajna
- vrlo fleksibilna tehnologija izrade koja omogućuje prilagodbu dizajna prema određenom nivou sigurnosti koju zahtjeva kupac
- aplikacija kinegrama® se ograničava na visoko zaštićene dokumente i ne koristi se za aplikaciju na komercijalne proizvode za razliku od hologram
- moguća integracija strojno čitljivih elemenata

Kinegrami® mogu biti izrađeni u obliku potpuno metaliziranih, djelomično metaliziranih i potpuno de-metaliziranih folija. U izradi putovnica, najčešće se koriste potpuno de-metalizirane kinegram® folije jer su transparentne te mogu služiti za djelomično prekrivanje fotografije ili potpuno prekrivanje identifikacijske stranice, što predstavlja vrlo dobar zaštitni element.

Slika 16 – Transparentni Kinegram® na identifikacijskoj stranici putne isprave RH (izvor: AKD)

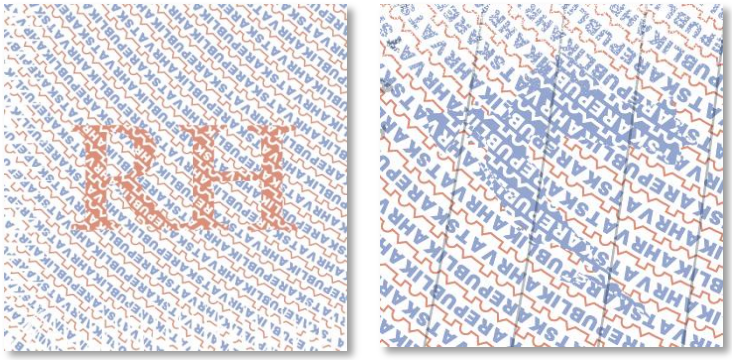
Kontrolna (sekundarna) slika nosioca putne isprave

U svrhu vizualne zaštite osobnih podataka nosioca putne isprave na identifikacijsku stranicu moguće je dodatno postaviti i drugu sliku nosioca putne isprave. Druga kontrolna slika (eng. *ghost image*) može se izraditi laserskim graviranjem ili mikroperforacijom, tehnikom ink jet UV tiska ili uporabom jedne vrste hologrami - identigram.

Slika 17 – Laserski mikro-perforirana sekundarna slika nizozemske putovnice vidljiva u proziru

Mikrotisak

Reprodukcija vrlo sitnog teksta koji je „golom“ oku neprepoznatljiv, a moguće ga je identificirati upotrebom povećala. Njegovo zaštitno svojstvo očituje se u nemogućnosti fotokopirnih uređaja i kompjuterskih skenera da ga reproduciraju na originalan (istovjetni) način. Smještajem ovog zaštitnog elementa na skrivena mjesta u putnoj ispravi osigurava se vrlo dobra zaštita od pokušaja krivotvorenja. Dodatni zaštitni element mikrotiska su namjerne greške u tekstu ili strukturi koje osiguravaju autentičnost pri eventualnim pokušajima krivotvorenja. Mogućnosti programskih aplikacija za generiranje mikrotiska su mnogobrojne, pa tako mikrotisak može biti izrađen u verzijama mikrotiska u negativu, pozitivu te varijabilnog mikrotiska, gdje je font unutar samog teksta promjenjive veličine.



Slika 18 - Elementi mikrotiska u putnoj ispravi RH (izvor: AKD)

Guilloche uzorci

Zaštitni element koji se sastoji od vrlo složene strukture finih linija formiranih prema principu matematičkih algoritama uz upotrebu specijalnih vektorskih programa. Zbog svoje složene kompozicije višebojnih tankih linija, nemoguće ih je reproducirati pomoću fotokopirnih i skenerskih uređaja zbog njihova ograničenja spram rezolucije. Osim svog zaštitnog svojstva, različite strukture *guilloche* uzoraka (*rosette*, *vignette* i sl.) pružaju i vrlo zanimljiv estetski dojam i djeluju kao antikopirajući uzorak (*eng. antiscann pattern*). Guilloche uzorci mogu biti izrađeni u negativu i pozitivu.

Slika 19 - Guilloche uzorci

Reljefne (taktilne) laminacijske strukture

Zaštitni element sličan ispupčenom laserskom graviranju s razlikom što ne nastaje tokom personalizacije putne isprave nego u postupku proizvodnje polikarbonatne stranice i nema obojenja. Motiv za trodimenzionalni opipljivi zaštitni element može biti slika i tekst, stoga se obično za putne isprave koriste simboli grba ili stihovi nacionalne himne. Može se očitovati i u djelomično, po određenom uzorku, matiranim dijelovima završnog sloja. Motiv za djelomično matirani završni sloj može biti slika i tekst (mikrotekst).

Slika 20 - Taktilne laminacijske strukture na PC identifikacijskoj stranici putne isprave RH(izvor: AKD)

MLI/CLI element

MLI je vodoravna rebrasta struktura na površini polimerne identifikacijske stranice koja prikazuje različite slike pri različitim kutovima gledanja. Slika je u navedenoj strukturi stvorena laserskim graviranjem.

MLI element proizveden je u toku procesa laminacije polimerne identifikacijske stranice uz upotrebu posebno izrađenih ploča za laminaciju.

Laserska zraka trajno ispisuje podatke pod različitim kutovima polimerne stranice na istom području, tako da nastaje dvostruka slika smještena jedna iznad druge.

Na području MLI-a se najčešće ispisuju podaci kao što su datum izdavanja u kombinaciji sa inicijalima korisnika kartice. CLI element za razliku od MLI-a sadrži okomite rebraste linije.

Slika 21 - MLI element na putnoj ispravi RH (izvor: AKD)

Taktilno lasersko graviranje

Laser za graviranje, tj. personalizaciju polimerne identifikacijske stranice putnih isprava ima svojstvo promjene specifične energije graviranja. Ukoliko se određeni podaci graviraju specifičnom energijom koja ovisi i o svojstvu polimera, dolazi do efekta uzdizanja graviranih elemenata, stvarajući tako opipljivi trodimenzionalni zaštitni element.

Slika 22 - Taktilni tekst na osobnoj iskaznici RH(izvor: AKD)

Sakrivena slika (eng. *Hidden image*)

Specifični zaštitni element trećeg nivoa sigurnosti nevidljiv bez specijalnih pomagala. Element se generira laserskim graviranjem specifičnog kuta rastera i postaje vidljiv tek

primjenom posebnih leća s polarizacijskim svojstvima. Unutar slike nosioca putnog dokumenta najčešće se upisuje ime i prezime i datum isteka valjanosti ili datum rođenja ili neki drugi numerički podatak.

OLED

Razvoj novih zaštita visoko-zaštićenih dokumenata danas je usmjeren uglavnom ka implementaciji novih elektroničkih tehnologija u papirnati ili polimerni medij. Naročito se to odnosi na segment zaštitnih elemenata I. razine zaštite, tj. onih zaštitnih elemenata koji se mogu detektirati jednostavnom vizualnom metodom bez uporabe specijalnih pomagala. Težnje na ovom području uglavnom su usmjerene ka implementaciji tzv. optičkih zaslona (eng. *optical display*) koji pružaju efekt animacije slike ili neke druge vrste informacije, senzora koji mogu služiti kao skeneri za privremeno pohranjivanje biometrijskih informacija poput otisaka prstiju i sl.

Tvrtka Bundesdruckerei GmbH iz Njemačke, promovira svoj izum iz grupe OLED zaslona (*organic light emitting device*) na bazi polu-vodljivog organskog materijala i polimera koji je integriran u tijelo polimerne identifikacijske stranice ili kartice. Organski materijal nalazi se u sendviču dvije elektrode i emitira svijetlost kada mu se dovede napon. Takav organski materijal je u konekciji sa beskontaktnim čipom i antenom koji su integrirani u središtu strukture polimerne kartice ili identifikacijske stranice, a koji putem elektromagnetskih valova šalju informaciju na zaslon. Tehnologija je još uvijek u procesu razvoja i usavršavanja te nije doživjela masovnu produkciju vezanu uz izdavanje nekog od identifikacijskih dokumenata.

Slika 23 – OLED zaslon tvrtke Bundesdruckerei GmbH

3D Photo ID

Tvrtka Sagem Identification promovira svoj zaštitni element 3D photo ID. 3D photo ID predstavlja trodimenzionalnu sliku nositelja dokumenta izrađenu tehnikom laserskog graviranja na površini mikronskih leća polimerne kartice ili identifikacijske stranice. Kako bi se kreirao ovaj zaštitni element neophodno je postojanje 4 fotografije nositelja dokumenta koje su izrađene odjedanput iz različitih kutova. Sve 4 slike su personalizirane tehnikom laserskog graviranja na površinu mikronskih leća, svaka pod svojim kutom graviranja na istom polju layout-a (jedna iznad druge). Ovaj zaštitni element sličan je MLI/CLI elementu koji je izrađen prema sličnom principu, razlika se očituje je u veličini leća koje su u ovom slučaju puno sitnije i na dodir potpuno neopipljive, te u broju različitih slika graviranih na istom polju.

Slika 24 – 3D Photo na ID kartici (gore); istovremeno uzimanje 4 fotografije (dolje)

8.2. Stranica sa podacima nositelja putovnice ili identifikacijska stranica putovnice

Nominalna dimenzija identifikacijske stranice definirana je ISO/IEC 7816 standardom, te preuzeta u ICAO Doc 9303, a iznosi 88 x 125 mm. Stranica se sastoji od 2 osnovna polja u koja se nekom od odabranih personalizacijskih metoda upisuju podaci o nositelju putovnice i to:

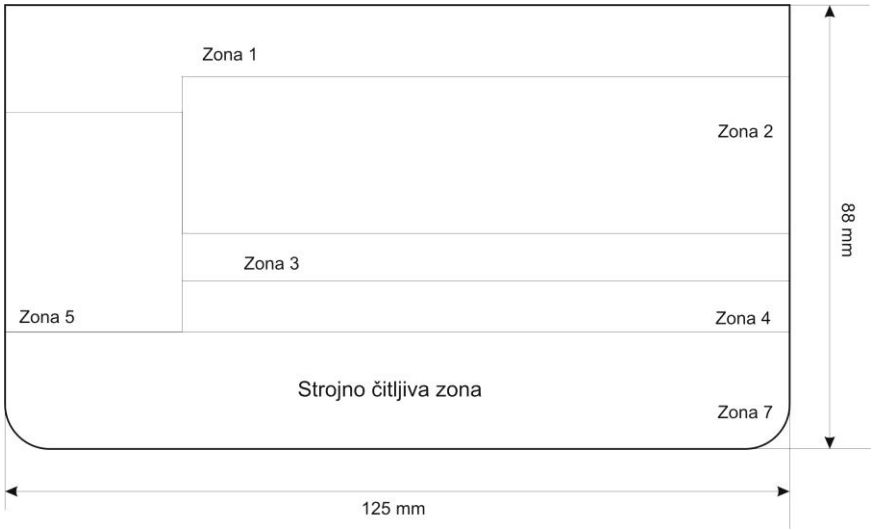
- VIZ (*vizual zone* – vizualna zona)
- MRZ (*machine readable zone* – strojno čitljiva zona)

VIZ polje sadrži obavezne podatke o nositelju, uključujući sliku i potpis, izdavatelju i vrsti putne isprave, podijeljene u 6 zona.

MRZ područje sadrži strojno čitljive podatke definirane zonom 7, ispisane u 2 reda. Strojno čitljiva zona sadrži podatke o nositelju putovnice u formatu koji je strojno čitljiv od strane čitača dokumenata. Svaka linija sadrži 44 znaka unutar kojih su spremljene slijedeće informacije: ime, broj putovnice, nacionalnost, datum rođenja, spol, datum isteka putovnice i osobni identifikacijski broj. Postoji također i prostor za upis opcionalnih, dodatnih informacija po izboru svake države.

Za sigurnost dokumenta je vrlo važna kvaliteta ispisa strojno čitljive zone jer je ona jedini element putovnice (koja ne sadrži beskontaktni čip) koji se strojno očitava i provjerava. Sastoji se od OCR-B strojno čitljivog fonta koji je specificiran u ISO 1073-II standardu te niza alfanumeričkih znakova koji uključuju slova od A – Z, brojeve od 0 do 9 i znaka <. Budući da se na graničnim prijelazima nalaze čitači putovnica različitih brendova i proizvođača važno je da je i čitač sukladan navedenom standardu kako bi se ostvarila odgovarajuća verifikacija putovnice.

Pravilo generiranja strojno čitljive zone definirano je također dokumentom ICAO Doc 9303.



Slika 25 – Layout zona podataka na identifikacijskoj stranici

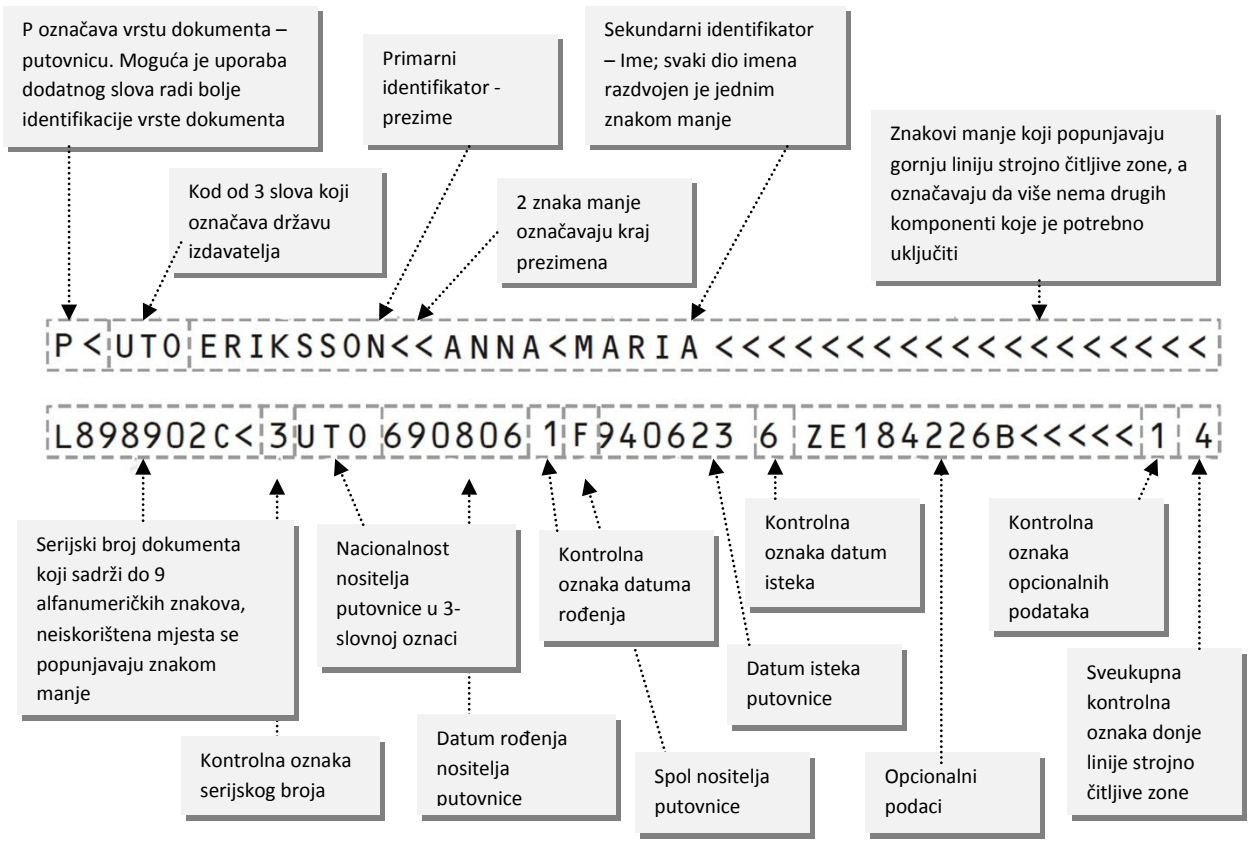
Slika 26 prikazuje skicu smještaja pojedinih zona na identifikacijskoj stranici putnog dokumenta, pa iako postoji još nekoliko mogućnosti pozicioniranja zona koje ICAO Doc 9303 nudi, ovo je prikaz zona koji je najčešće korišten u praksi.

Zone za vizualnu inspekciju podataka nosioca putne isprave sadrže slijedeće informacije:

Zona	Podatak
Zona 1	Država koja izdaje dokument
	Vrsta putne isprave
	Oznaka dokumenta
	Kod države koja izdaje dokument
	Serijski broj putne isprave
Zona 2	Ime i Prezime
	Državljanstvo
	Datum rođenja
	Jedinstveni broj nositelja putne isprave
	Spol
	Mjesto rođenja
Zona 3	Datum izdavanja putne isprave
	Državno tijelo koje je izdalo putnu ispravu
	Datum isteka valjanosti putne isprave
Zona 4	Vlastoručni potpis nositelja putne isprave
Zona 5	Slika nositelja putne isprave

Tablica 11 – Podaci zona vizualnog dijela putne isprave

Slika 26 – Prikaz elemenata podataka strojno čitljive zone



Izradila: Željka Stražnicky, lipanj 2011.

8.3. Specifikacije elektroničke putovnice

8.3.1. Korice

Elektronička putovnica primjenjuje sve navedene specifikacije strojno čitljivih putovnica ali dodaje i neke nove.

Svaka strojno čitljiva putovnica s beskontaktnim čipom, koja sadrži elektroničke podatke nositelja putne isprave pripremljene u skladu sa zahtjevima ICAO-a, na prednjoj strani korica, osim naziva putne isprave, naziva države i obilježja države, mora sadržavati slijedeći simbol prikazan na slici 27 [10].

Slika 27 - Međunarodni znak koji označava elektroničku putovnicu s beskontaktnim čipom

Simbol e-putovnice otiskuje se tehnikom foliotiska istom folijom koja se koristi i za otiskivanje ostalih obaveznih tekstualnih elemenata (naziv države, naziv dokumenta).
Za veličinu znaka u standardu ICAO predviđa 2 dimenzije:

a) 9 mm x 5,25 mm (A)
b) 7,2 mm x 4,2 mm (B)

Osim simbola A, ICAO je ostavio mogućnost aplikacije simbola B veličine 7,2 mm x 4,2 mm. Izbor između dvije dimenzije simbola za putovnice sa čipom omogućene su isključivo iz dizajnersko-estetskih razloga. Ukoliko podaci na putnoj ispravi otisnuti foliotiskom zauzimaju puno prostora na koricama, predviđena je aplikacija simbola B.

Obzirom na mogućnost aplikacije manjeg simbola B i većeg simbola A, navedene simbole moguće je smjestiti u gornjem ili donjem dijelu prednje stranice korica putne isprave, unutar predviđenih gabarita definiranih u standardu.

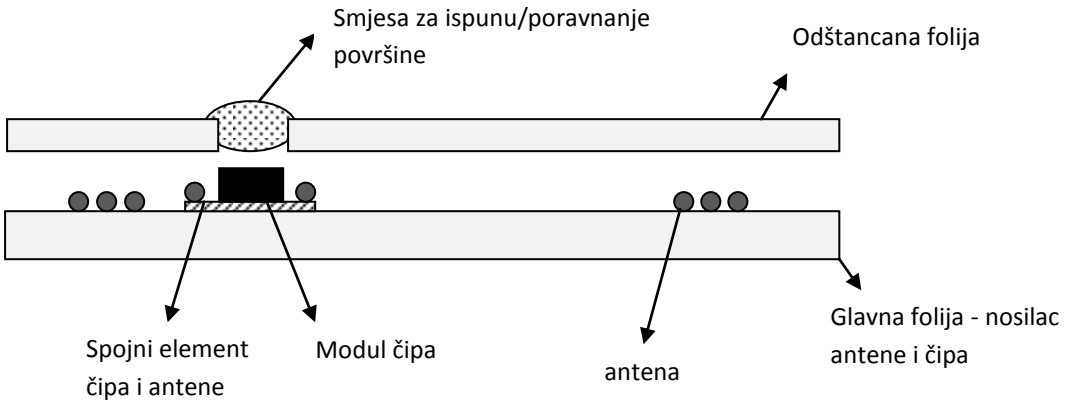
8.3.2. Smještaj beskontaktnog čipa u putovnici

Smještaj beskontaktnog čipa i antene u putovnici prema ICAO standardu može biti unutar [10]:

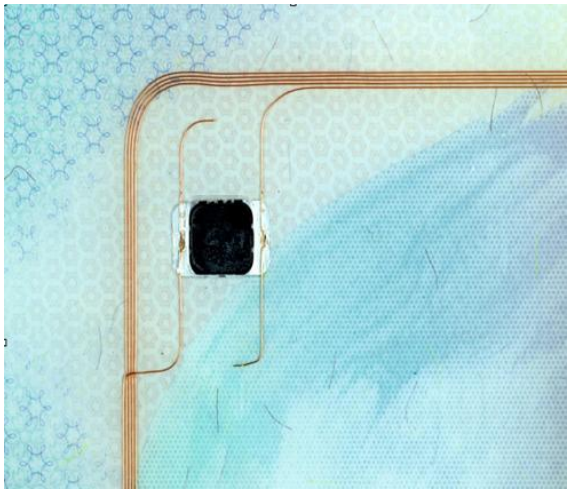
a) identifikacijske stranice
b) centra knjižnog bloka
c) korica putovnice

Bez obzira o kojoj se od ove 3 pozicije radi beskontaktni čip sa antenom mora biti integralni dio svakog od navedenih dijelova te zaštićen na odgovarajući način kako bi se onemogućilo njegovo slučajno oštećivanje.

Komponenta strukture koja „nosi“ beskontaktni čip i antenu naziva se *inlet/inlay* (engl. *let in* – staviti u, *lay in* – leći u) ili *prelam* (eng. *pre-lamination* – pred-laminacijski) i nalazi se u samom središtu ukupne strukture korica ili identifikacijske stranice kako bi bila maksimalno zaštićena od vanjskih mehaničko-kemijskih utjecaja. Struktura *inleta* ili *prelama* u svom presjeku najčešće izgleda kao na slici 28.



Slika 28 – Struktura inleta/prelama



Slika 29 – Spoj antene i čipa

Postoji nekoliko različitih tehnologija proizvodnje i apliciranja antene na glavnu foliju koja ima ulogu njenog nositelja u strukturi inleta. Oblik i veličina (geometrija) antene kao i smještaj beskontaktnog čipa određen je električkim karakteristikama beskontaktnih sustava za koji se koriste, zahtjevima vezanima uz kapacitet, veličinu otpora i induktivitet. Primijenjena veličina antene u inletima za e-putovnice jednaka je veličini beskontaktnih antena za *smart* kartice, a kreće se u rasponu formata ID1 (86 x 54 cm).

Postojeće tehnologije nanašanja antene na foliju su:

- Bakrena žica sa izolacijskim lakom navijena na okruglu jezgru sa koje se aplicira na foliju i spaja termičkim postupkom. Ovaj postupak je vrlo kompleksan i rijetko korišten.
- Aplikacija izolirane žice na foliju uz pomoć ultrasoničnog varenja pri čemu je bakrena žica lagano utopljena u plastični materijal. Ovaj postupak je vrlo brz i fleksibilan te omogućava vrlo dobro podešavanje geometrije antene.
- Jetkanje antene iz bakrenog sloja koji je nanesen na punu površinu plastične folije specijalnim tehnikama laminacije. Nakon laminacije bakrenog sloja na njega se nanosi fotoosjetljivi sloj i osvjetljava kroz foto-masku koja sadrži strukturu antene. U postupku kemijskog razvijanja, ne-osvijetljeni dio fotoosjetljivog sloja se uklanja, a suvišan dio bakrenog sloja jetka. U posljednjem koraku osvijetljeni dio sloja se uklanja, a ispod njega ostaje očekivana struktura antene. Ovo je jedan od najčešće korištenih postupaka izrade antene te je dobra alternativa postupku sa ultrasoničnim varenjem.
- Otisnuta antena tehnikom sitotiska upotrebom specijalnih pasta na bazi srebra. U usporedbi sa jetkanom antenom u ovom postupku se javlja problem izrade vrlo finih vodljivih elemenata zbog vrlo velikih pigmenata sitotiskarskih boja. Iako je ovaj postupak izrade antene najekonomičniji, javljaju se problemi vezani uz kvalitetu i mogućnost postizanja očekivanih električkih karakteristika povezanih s otporom.

8.3.3. Beskontaktni integrirani krug – beskontaktni čip

Globalna potreba za dodavanjem novih podataka u putovnicu, kao što su biometrijski, dovela je do neophodnosti uvođenja čipa kao dodatnog elementa za pohranu podataka. Kao najbolje rješenje pokazao se beskontaktni čip koji se zbog svojih tehničkih značajki najlakše implementira i nudi bolje komunikacijske performanse od kontaktnih čipova.

Beskontaktni čip je samo jedan dio sustava koji se sastoji od samog čipa, pripadajuće mu antene, te RF (*radio frequency*) čitača koji komunicira sa čipom i ujedno je izvor napajanja za čip.

Beskontaktni čip je pasivan element jer nema vlastiti izvor napajanja. Umjesto vlastitog izvora napajanja koristi se vanjska pobuda koja elektromagnetskom indukcijom preko čipu spojene antene inducira struju potrebnu za rad čipa. Podaci se između čipa i čitača razmjenjuju bez njihovog fizičkog kontakta, u radnom frekvencijskom pojasu.

čitač

Kartica sa beskotaktnim čipom i antenom

Slika 30 – Čitač i beskontaktna kartica

Prema ICAO specifikaciji, čip koji se ugrađuje u putovnicu treba biti u skladu sa standardima ISO/IEC 14443 tip A/B i ISO/IEC 7816-4.
Standard ISO/IEC 7816-4 specificira zahtjeve za pristup podacima stoga je potrebno odabrati čip čiji operativni sustav zadovoljava ovaj standard.

Prostor za pohranu podataka mora biti dovoljnog kapaciteta iz slijedećih razloga:

- kako bi se osigurao prostor za aplikacije koje treba ugraditi u čip (LDS - *Logical Data Structure*) aplikaciju,
- zbog fleksibilnosti,
- biometrijskih podataka,
- tekstualnih podataka,
- certifikata,
- kriptografskih ključeva,
- brzine čitanja moraju biti što veće kako bi se osigurala praktičnost u korištenju na graničnim prijelazima i kod ostalih službenih kontrola dokumenata.

Mnoge su mogućnosti beskontaktne tehnologije, a neke od njih su [11]:

- **Visoka propusnost i brza transakcijska vremena**. Beskontaktna tehnologija omogućuje visoke brzine prijenosa podataka na graničnim prijelazima ili nekim drugim mjestima provjere.
- **Visoki stupanj zaštite podataka**. Beskontaktni čipovi imaju sposobnost enkripcije podataka koji su pohranjeni u njemu, te enkripcije komunikacijske veze između čitača i čipa.
- **Visoka sigurnost čipa**. Beskontaktni čipovi imaju vrlo kompleksne ugrađene metode obrane od krivotvorenja.
- **Sofisticirani procesi obrade podataka u čipu**. Unutar samoga čipa moguće je odvijanje više različitih funkcija poput, pohrane podataka, enkripcije, dekripcije i dr.
- **Autentificiran i autoriziran pristup informacijama u čipu**. Čipovi imaju mogućnost zaštite pristupa pojedinim pohranjenim podacima te mogu zahtijevati autentifikaciju onoga tko

želi pristupiti podacima, provjeriti njegova prava pristupa i dozvoliti pristup (selektivno ili u cijelosti).

- **Pohranjivanje biometrijskih podataka i procesuiranje**. Zaštita pristupa biometrijskim podacima uz mogućnosti verifikacije netom uzetog biometrijskog podatka sa čitača te usporedbe sa onim pohranjenim u čipu. Pri tome je privatnost podataka osigurana jer pohranjeni biometrijski podatak ne napušta čip, a procesi usporedbe događaju se na samom čipu, a ne na čitaču.
- **Prikladnost korištenja**. Beskontaktna tehnologija se lagano i jednostavno koristi. Medij koji sadrži beskontaktnu tehnologiju nije potrebno ubacivati u uređaj, provlačiti kroz uređaj i nije zahtijevana specifična orijentacija.
- **Visoka trajnost i pouzdanost**.
- **Mogućnost korištenja u lošim uvjetima i prljavoj okolini**. Beskontaktna tehnologija je uvijek ugrađena unutar nekog od medija (kartice, knjižice i sl.), sprječavajući tako negativni utjecaj prašine, vode, hladnoće i dr.
- **Fleksibilnost ugradnje**. Beskotaktna tehnologija može biti ugrađena u razne oblike, poput plastičnih kartica, satove, putne dokumente, privjeske, narukvice, kapsule i sl., ovisno o željenoj funkcionalnosti krajnjeg proizvoda.
- **Široko područje primjene**. Ovisno o željenoj funkcionalnosti, beskontaktna tehnologija može se koristiti u obliku platnih – bankarskih kartica, kartica za fizički pristup prostorima, kao identifikacijske kartice sa visokom razinom zaštite podataka, cestovne kartice i sl.
- **Tehnologija bazirana na međunarodnim standardima**. Beskontaktna tehnologija usklađena je sa nizom ISO standarda. Globalna interoperabilnost osigurana je unutar radio frekvencijskog područja od 13,56 Hz koja je dostupna širom svijeta. Mnogi proizvodi usklađeni sa navedenim standardom su dostupni na tržištu od strane više izdavača koji mogu ponuditi svoje gotove funkcionalne aplikacije zajedno sa opremom i softverom za čitanje i obradu.

8.3.4. 1. generacija elektroničkih putovnica Vs. 2. generacija elektroničkih putovnica

Novi zahtjevi definirani ICAO standardom te regulativom vijeća Europe iz 2004.god. mogu se sažeti kako slijedi:

- Putovnice i putni dokumenti moraju imati integriran visoko zaštitni medij za pohranu informacija u elektroničkom obliku – beskontaktni čip i pripadajuću antenu.
- Beskontaktni čip mora biti usklađen sa ISO/IEC standardom 14443 tip A ili B.
- Operativni sustav na čipu mora odgovarati ISO/IEC standardu 7816-4.
- Udaljenost čitanja čipa do 10 cm.
- Minimalna memorija čipa (EEPROM - *Electrically Erasable Programmable Read-Only Memory*) od 32 kB, sa preporukom od 64 kB.

- Čip ne smije imati statični jedinstveni identifikator (UID – *Unified identifier*), već varijabilni koji pri svakom čitanju pokazuje drugačije vrijednosti.
- Čip mora imati standardiziranu aplikaciju izrađenu prema ICAO specifikacijama [10] i nazvanu LDS (*Logical Data Structure*) aplikacija.
- Pored uobičajenih tekstualnih podataka ispisanih na identifikacijskoj stranici, čip mora sadržavati sliku lica u formatu JPEG 2000, te 2 otiska prsta u WSQ formatu te digitalni potpis.
- Povjerljivost podataka mora biti osigurana autentifikacijskim protokolima i kriptiranom komunikacijom definiranim standardom.

Kako su u Europskoj Uniji obavezne elektroničke putovnice 2. generacije, a u SAD-u i ostatku svijeta još uvijek elektroničke putovnice 1. generacije, to su i specifikacije vezane uz tip podataka te autentifikacijske mehanizme koje osiguravaju povjerljivost podataka, različiti kod jedne u odnosu na drugu. Kratkom skicom su prikazane osnovne razlike u navedenim tipovima putovnica.

1. GENERACIJA E-PUTOVNICA		
Podaci pohranjeni u čipu	Strojno čitljiva zona	OBAVEZNO
	Slika lica	OBAVEZNO
	Digitalni potpis	OBAVEZNO
Autentifikacijski mehanizam	Pasivna autentifikacija (PA)	OBAVEZNO
	Osnovna kontrola pristupa BAC)	OBAVEZNO
	Aktivna autentifikacija (AA)	OPCIONALNO

Tablica 12 – Popis zahtjeva vezanih uz podatke i autentifikacijske mehanizme 1. generacije e-putovnica

2. GENERACIJA E-PUTOVNICA		
Podaci pohranjeni u čipu	Strojno čitljiva zona	OBAVEZNO
	Slika lica	OBAVEZNO
	Digitalni potpis	OBAVEZNO
Autentifikacijski mehanizam	Pasivna autentifikacija (PA)	OBAVEZNO
	Osnovna kontrola pristupa BAC)	OBAVEZNO
	Aktivna autentifikacija (AA)	OPCIONALNO
	Proširena kontrola pristupa (EAC)	OBAVEZNO u EU

Tablica 13 – Popis zahtjeva vezanih uz podatke i autentifikacijske mehanizme 2. generacije e-putovnica

8.3.5. LDS aplikacija

Kako bi se osigurala globalna interoperabilnost pri strojnom čitanju pohranjenih podataka u čipu putovnice, ICAO je inicirao postupak razvoja standardizirane čip aplikacije koja bi imala

unificirani način organizacije podataka primjenom tehnologije proširivog kapaciteta. Takva aplikacija nazvana je LDS aplikacija – *Logical Data Structure*.

Niz obaveznih i opcionalnih elemenata podataka je definiran unutar LDS aplikacije kako bi se osiguralo ispunjenje globalnih zahtjeva za provjeru e-putovnica. Podaci unutar aplikacije grupirani su po grupama DG (*Data Group*), koje se protežu od DG1 – DG19. Neke od DG grupa još nisu u uporabi a predviđene su za buduću uporabu (grupe od DG17 – DG19). Sadržaj elemenata pojedine grupe prikazan je na slici 31 i 32.

			ELEMENTI PODATAKA	
Podaci iz strojno čitljive zone		**DG1**	Tip dokumenta	**OBAVEZNI PODACI**
			Država izdavatelj ili organizacija	
			Ime	
			Broj dokumenta	
			Kontrolna oznaka – na broj dokumenta	
			Nacionalnost	
			Datum rođenja	
			Kontrolna oznaka – na datum rođenja	
			Spol	
			Datum isteka putovnice	
			Kontrolna oznaka – na datum isteka	
			Opcionalni podaci (prema izboru države)	
			Skupna kontrolna oznaka	
Kodiran identifikacijski element	Globalni element razmjene	**DG2**	Kodirana slika lica	
	Dodatni elementi	**DG3**	Kodirani otisci prstiju	
		DG4	Kodirana šarenica oka	
Prikazani identifikacijski elementi		**DG5**	Prikazana slika lica	**OPCIONALNI PODACI**
		DG6	Rezervirano za buduće korištenje	
		DG7	Prikazani potpis	
Kodirani sigurnosni elementi		**DG8**	Elementi podataka	
		DG9	Struktura podataka	
		DG10	Sadržaj podataka	
		DG11	Dodatni osobni podaci (opcionalno)	
		DG12	Dodatni podaci o dokumentu (opcionalno)	
		DG13	Opcionalni podaci (DS certifikat)	
		DG14	Javni ključ proširene kontrole pristupa	
		DG15	Javni ključ aktivne autentifikacije	
		DG16	Podaci osobe koja potvrđuje valjanost putovnice	

Tablica 14 – Prikaz podataka unutar LDS aplikacije [10]

DG17	Potvrda prolaska kroz automatiziranu granicu
DG18	Elektronička viza
DG19	Podaci o putovanjima

Tablica 15 – Prikaz podataka za buduću uporabu unutar LDS aplikacije [10]

Osim obaveznih podataka navedenih na slici LDS aplikacije, obavezni su i elementi podataka PKI infrastrukture koja čini okosnicu čitavog sustava izdavanja i provjere e-putovnica. Elementi podataka PKI infrastrukture vezani su uz dokazivanje integriteta i autentičnosti podataka, a više će biti objašnjeni u poglavlju PKI infrastrukture.

8.4. Proizvodnja e-putovnica

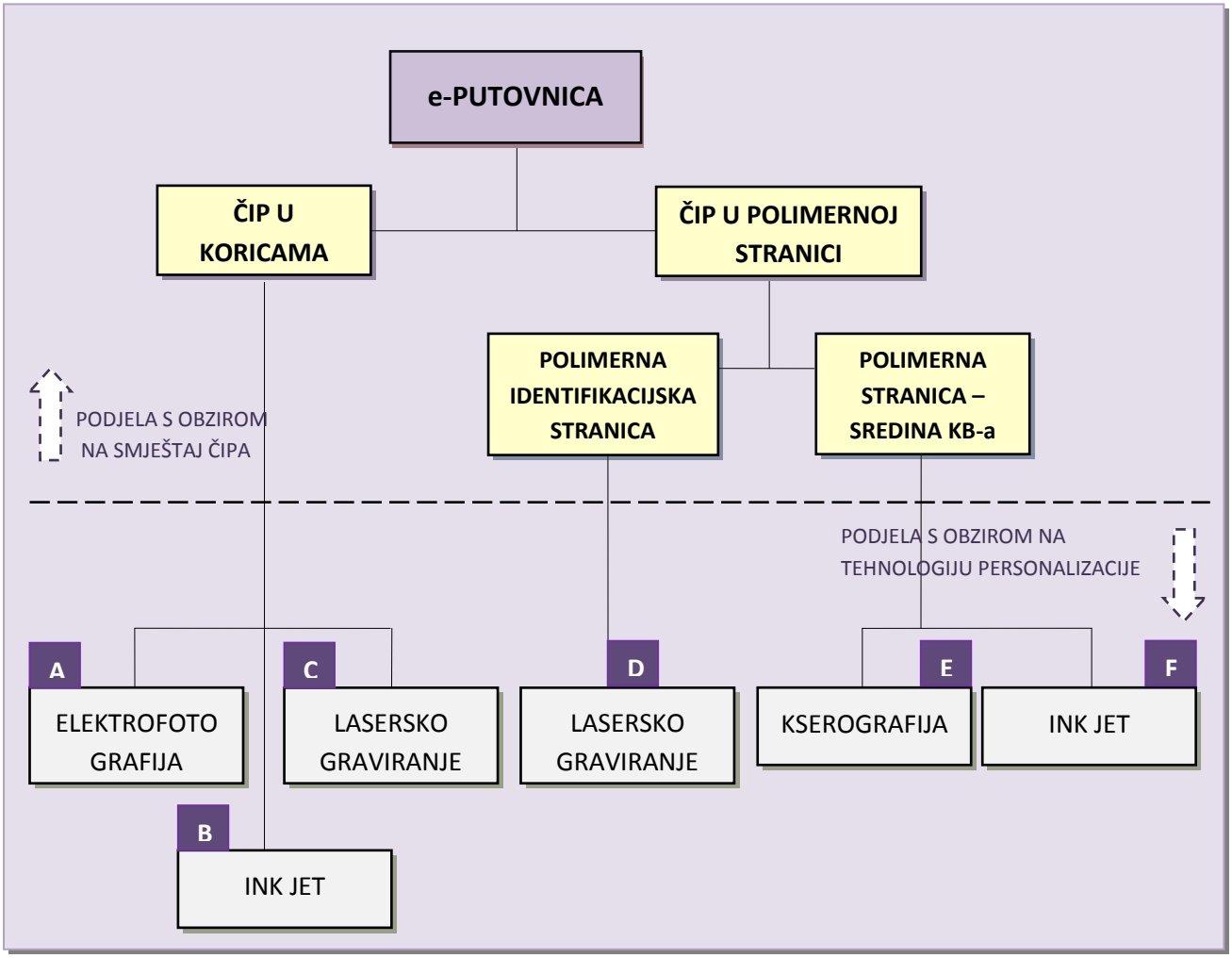
Osnovne komponente svake ICAO standardizirane putovnice su:

- Korice (*e*-korice)
- Predlist/zalist
- Identifikacijska stranica (polimerna identifikacijska stranica s čipom)
- Knjižni blok

Svaka od ovih komponenata putovnice čini jedinični poluproizvod sa svojim jedinstvenim proizvodnim tijekom, zakonitostima i tehnikama izrade specifičnim upravo za tu komponentu. Pojavom elektroničkog nosioca podataka, najveće promjene u procesu proizvodnje putovnica doživjele su korice i identifikacijska stranica putovnice. Njihova transformacija očitovala se u potrebi integracije do tada konvencionalnog papirnog ili plastičnog materijala sa novim materijalima na metalnoj osnovi koji čine antenu i čip. Stoga su najveći izazovi u proizvodnji putovnica u prvom redu bili kvalitetni spojevi te dvije grupe fizikalno-kemijski nekompatibilnih materijala, sa vijekom trajanja od 10 god. pri normalnoj uporabi putovnice. Iako se navedene osnovne komponente putovnice razlikuju svojim proizvodnim procesima izrade, spajaju se/uvezuju u gotovu knjižicu putovnice prolazeći kroz standardne faze linijskog načina proizvodnje putovnica koje su zajedničke gotovo svim svjetskim proizvođačima putovnica. Razlog tome je dominacija 2 velika proizvođača na tržištu strojeva za uvez putovnica: *Kugler Womako GmbH.* i *UNO Seisakusho Co. Ltd.*

Glavne različitosti u proizvodnim konceptima izrade putovnice među proizvođačima uglavnom se manifestiraju u procesu personalizacije, odnosno dodavanja osobnih podataka korisnika i drugih specifičnih podataka u knjižicu putovnice. Te su različitosti uglavnom povezane sa primijenjenim tehnikama personalizacije, ali i odabranim smještajem čipa u putovnici.

Osnovna podjela e-putovnica obzirom na primijenjenu tehniku personalizacije te smještaj čipa i antene može se prikazati kao na slici 31.

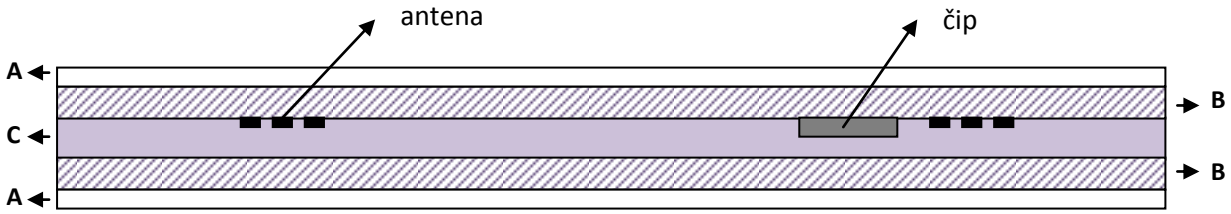


Slika 31– Podjela e-putovnica s obzirom na smještaj čipa te tehniku personalizacije

Kada se govori o integraciji čipa i antene unutar strukture korica ili polimerne stranice koja se pojavljuje u obliku identifikacijske stranice ili zasebne *bianco* (neotisnute) stranice u središtu knjižnog bloka, postoji više načina izrade koji su ovisni o samom proizvođaču integrirane komponente i koji čine svojevrsnu proizvođačku tajnu višeslojne strukture materijala.

Prilikom izrade polimerne identifikacijske stranice ili e-korica primjenjuju se vruća ili hladna laminacija materijala. Vrućom laminacijom izrađuju se polimerne stranice kombinirajući djelovanje temperature i pritiska simultano. Kod izrade elektroničkih korica, koje se uglavnom izrađuju od papirnih materijala (iako postoje slučajevi kombinacije papirnih i polimernih materijala), uglavnom se primjenjuje tehnika hladne laminacije (zbog kemijsko-fizikalnih svojstava papira), gdje se uporabom ljepila i postupkom prešanja slojevi materijala spajaju u jednu strukturu.

Primjer jedne od jednostavnijih struktura polimerne stranice koja sadrži čip i antenu, te ukupno 5 slojeva termo-plastičnih materijala prikazana je na slici 32.



Slika 32 – Bočni prikaz strukture polimerne stranice sa integriranim čipom i antenom (A – transparentni završni sloj, tzv. overlay, B – ne-transparenti tiskovni sloj, tzv. jezgra, C – inlet ili prelam)

Procesom vruće laminacije različiti termoplastični slojevi međusobno prodiru jedni u druge čineći tako kompaktnu strukturu koju nije moguće, bez destrukcije, naknadno odvojiti na njene sastavne dijelove. Jedan od razloga zašto je proces izrade identifikacijskih stranica evoluirao sa papirne osnove na plastičnu je upravo specifičnost izrade u kojem su tiskovni elementi sadržani u dubljim slojevima strukture čime je ukupna razina zaštite podignuta na viši nivo.

Na tržištu postoje različite vrste termo-plastičnih materijala, a da bi bili korišteni u izradi polimernih identifikacijskih stranica putovnice moraju zadovoljiti kriterije unutar kategorija:

- Mogućnost laminacije
- Dimenzionalna točnost
- Mogućnost otiskivanja
- Optička kvaliteta i konstanta obojenja
- Mehanička čvrstoća
- Životni vijek
- Termička stabilnost
- Otpornost na vlagu
- Otpornost na otapala
- Anti-statično svojstvo
- Kompatibilnost s okolišem za vrijeme proizvodnje i svakodnevne uporabe

Visoki zahtjevi u izradi polimernih identifikacijskih stranica determinirali su tržišnu dominaciju dvije grupe materijala, polikarbonata – PC i polietilena tereftalat – PET.

Međutim, u izradi polimernih identifikacijskih stranica polikarbonat prednjači, zbog čega je u praksi postalo uobičajeno čitavu kategoriju polimernih identifikacijskih stranica u kojima je smješten čip sa antenom nazivati polikarbonatnim identifikacijskim stranicama (eng. *PC data page*).

Pojavom polikarbonatne identifikacijske stranice bilo je potrebno osmisliti adekvatne metode i materijale za njeno spajanje sa ostatkom knjižnog bloka.

Dio takve polimerne identifikacijske stranice koji se uvezuje u knjižni blok naziva se zglobni materijal ili umetak (*hinge*). Umetak, odnosno spoj polimerne stranice s ostatkom knjižnog

bloka čini vrlo osjetljivu točku putovnice jer mora pružati dovoljnu čvrstoću kako bi držao višestruko težu stranicu ali i dovoljno fleksibilan kako ne bi puknuo upravo zbog te iste težine. Zbog toga je tehnologija spajanja umetka sa ostatkom identifikacijske stranice najčešće zaštićena patentom od strane pojedinog proizvođača koji nudi polimerne identifikacijske stranice kao jedan od svojih proizvoda. Tako na tržištu postoje različite tehnologije spajanja umetka sa ostatkom identifikacijske stranice, od tehnologije ultrasoničnog zavarivanja sa polimernim umetkom do tehnologije mehaničkog i kemijskog spajanja polimerne stranice sa umetkom od tkanine ili papira.

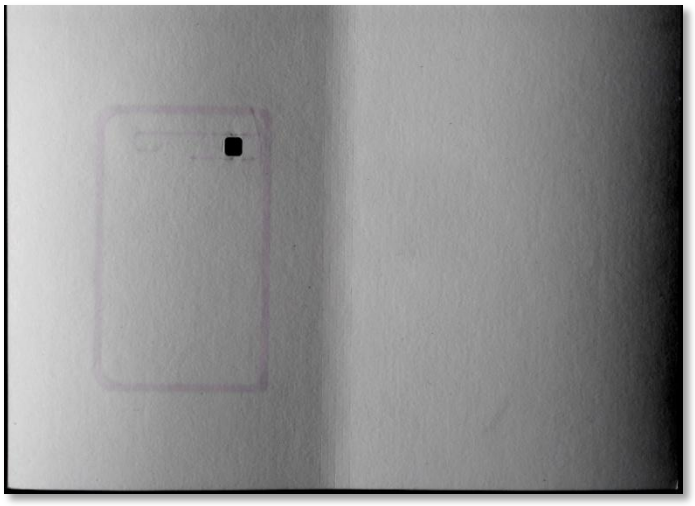
Slika 33 – PC stranica i umetak (izvor: AKD)

Polimerna identifikacijska stranica najčešće je debljine ≤ 1 mm, te sačinjena i do 10-ak slojeva polimera. Svaki o polimernih slojeva identifikacijske stranice ima svoju ulogu u procesu izrade kompaktne polimerne stranice, a čak nekoliko slojeva mogu imati funkciju nositelja nekog od zaštitnih elemenata, čime se zaštita stranice proteže kroz nekoliko nivoa debljine stranice.

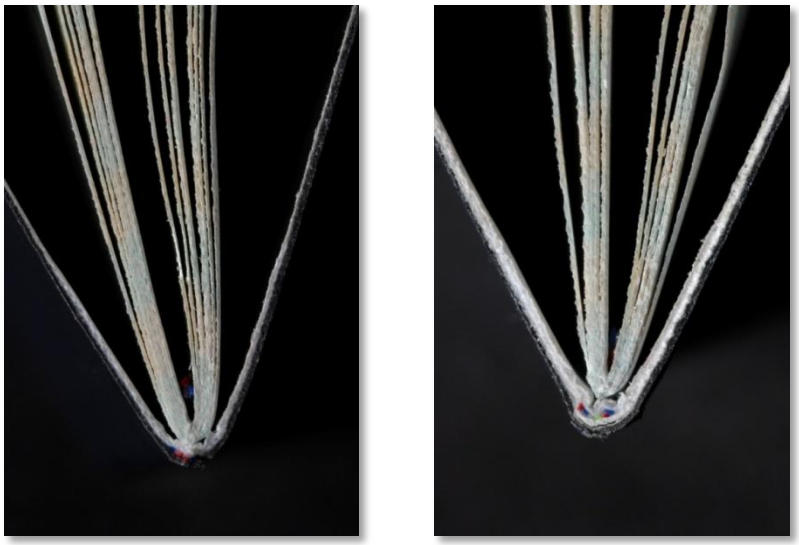
Slika 34 – Skica višeslojne PC stranice

Ukoliko su čip i antena smješteni u centru knjižnog bloka oni su također dijelom polimerne stranice koja najčešće nije identifikacijska. U tom slučaju identifikacijska stranica je najčešće papirna, a stranica sa čipom zasebna neotisnuta stranica u središtu putovnice – tzv. *bianco* polimerna stranica. U slučaju kada su čip i antena integralni dio korica tada su korice

načinjene od sintetičkih materijala, papirnatih materijala ili kombinacije jednih i drugih. Kao i polimerna identifikacijska stranica, korice su izrađene od više slojeva različitih materijala koji se mogu spajati tehnologijom vruće ili hladne laminacije. Čip sa antenom može biti dio prednjih korica, no najčešće je dio stražnjeg dijela korica kako bi bio što više zaštićen od mehaničkih utjecaja. Najčešće korištena antena je bakrena zbog svojih dobrih mehaničkih i provodljivih svojstava.



Slika 35 - e-korice (izvor: AKD)



Slika 36– Profil korica bez antene i čipa (lijevo) i korica sa antenom i čipom (desno) (izvor: AKD)

U slijedećoj tablici prikazana je usporedba 3 osnovna rješenja smještaja čipa i antene sa svojim prednostima i manama.

	Prednosti	Nedostaci
Polimerna identifikacijska stranica	✓ Polimerna stranica pruža mogućnost implementacije dodatnih zaštitnih elemenata koje je nemoguće ili složenije izraditi na papirnom mediju. ✓ Tehnologija individualizacije polimerne stranice - lasersko graviranja nudi mogućnost trajnog upisivanja podataka koje nije moguće izbrisati konvencionalnim metodama krivotvorenja. ✓ Lokacija čipa u PC stranici je teže vidljiva. ✓ Čip je je gotovo nemoguće odstraniti iz unutrašnjosti strukture stranice bez vidljivog i nepovratnog oštećivanja stranice.	✓ Zbog tvrdoće i nefleksibilnosti materijala, pod djelovanjem većih sila, može doći do pucanja i trajnog oštećenja čipa. ✓ Polimerna stranica mora biti izrađena na način da u svom sastavu sadrži površinu materijala pogodnu za ušivanje u knjižni blok. Zbog 2 različite vrste materijala (polimer i papir) koji se međusobno ušivaju, veza je osjetljivija i podložnija pucanju i odvajanju od ostatka KB-a ✓ Polimerna stranica zahtijeva tehniku laserske personalizacije koja je skuplja tehnologija personalizacije u odnosu na digitalne tiskarske tehnike. ✓ Cijena PC stranice je veća od cijene e-korice.
Polimerna *bianco* stranica - centar knjižnog bloka	✓ U centru može biti aplicirana i *tamper evident* naljepnica (naljepnica sa svojstvom delaminacije pri pokušaju odljepljivanja) sa antenom i čipom kao i *bianco* PC stranica.	✓ Identifikacijska stranica sa otisnutim podacima i strojno čitljivom zonom nositelja putovnice se nalazi zasebno na prvoj ili zadnjoj stranici putovnice, na predlistu ili zalistu putovnice, tj. odvojeno od čipa i antene što omogućuje jednostavniju zamjenu krivotvorenim segmentom bez utjecaja na čip ili obrnuto. ✓ Skupo rješenje, a ne nudi dodatne zaštitne elemente inkorporirane u polimernu stranicu.
e-Korice	✓ Sitotiskom otisnuta antena i aplicirani čip u koricama putovnice čine puno fleksibilniju i kompaktniju putovnicu u odnosu na putovnicu sa polimernom stranicom. ✓ Ekonomski prihvatljivije rješenje u odnosu na polimernu stranicu. ✓ Nije potrebno mijenjati postojeću tehnologiju personalizacije.	✓ Uporabom tehnologije sitotiska za izradu antene postavlja se pitanje kvalitete i izdržljivosti antene. ✓ U odnosu na polimernu stranicu postoji više razlika od dobavljača do dobavljača vezanih uz konstrukciju e-korica koje također mogu biti vrlo debele i nefleksibilne. ✓ Identifikacijska stranica je odvojena od komponente čipa i antene što omogućuje jednostavniju zamjenu krivotvorenim segmentom bez utjecaja na čip ili obrnuto.

Tablica 16 - Popis prednosti i nedostataka putovnica s obzirom na medij za smještaj čipa

Tehnike personalizacije

Elektrofotografija je jedna od najčešće korištenih tehnika personalizacije konvencionalnih putovnica u slučajevima centraliziranog sustava proizvodnje.

Ovom digitalnom tehnikom tiska otiskuje se arak papira koji čini identifikacijsku stranicu putovnice, koji se potom uvezuje kao jedan od poluproizvoda u gotovu putovnicu. Najčešće se prije procesa uveza oslojava zaštitnom hologramskom folijom tehnikom vruće laminacije preko cijele površine identifikacijske stranice, te kao njezin integralni dio biva ušivena u knjižni blok.

Zavisno o kojoj podvrsti elektrofotografije se radi tiskovni elementi ostvaruju se sustavom osvjetljavanja fotovodljivog bubnja/remena, obojavanja fotovodljivog bubnja/remena, prijenosa tonera na podlogu, fiksiranja tonera i čišćenja. Toner može biti praškasti ili tekući.

Ink jet je tehnika personalizacije koja se koristi i u centraliziranim i decentraliziranim sustavima proizvodnje putovnica.

Može se koristiti za tisak araka koji će činiti identifikacijsku stranicu ali češće za ispis identifikacijskih stranica već integriranih u tzv. *bianco* putovnicu (izrađena knjižica putovnice bez upisanih korisničkih podataka). U tom slučaju se u specifične tzv. personalizacijske strojeve, ubacuju gotove, uvezane *bianco* putovnice, otvaraju se na mjestu identifikacijske stranice i ispisuju ink-jet-om, a potom oslojavaju hologramskim slojem. U ovom slučaju hologramski sloj nije zajedno sa identifikacijskom stranicom integriran u hrbat knjižnog bloka putovnice, što može činiti povećani rizik od krivotvorenja identifikacijske stranice.

Lasersko graviranje

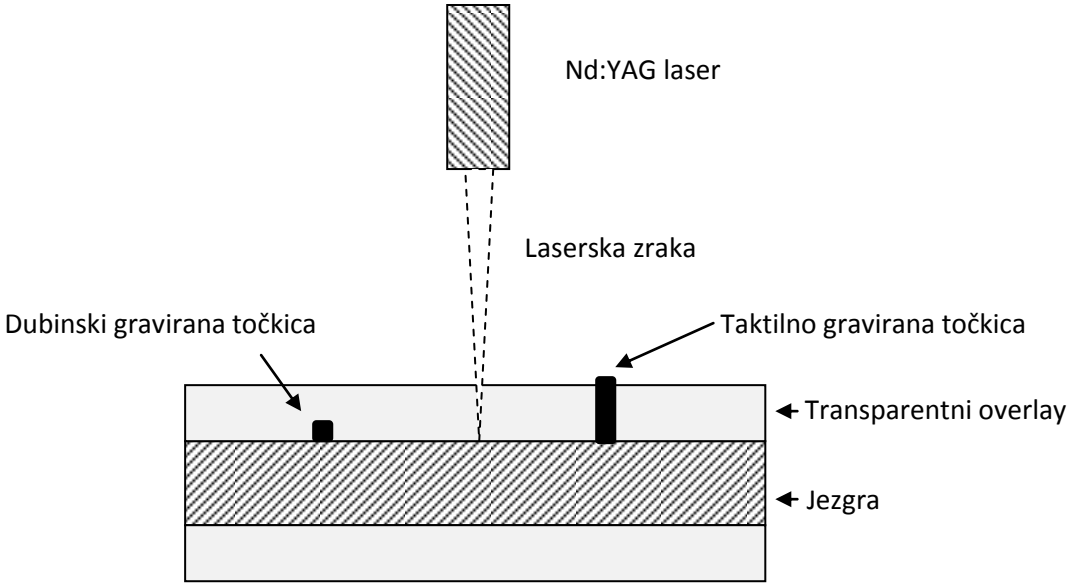
Pojavom polimernih, odnosno termo-plastičnih materijala u izradi identifikacijskih stranica, bilo je potrebno osmisliti nove tehnike personalizacije koje nisu više pripadale grupi standardnih tiskarskih tehnika, a jedna od takvih tehnika upravo je lasersko graviranje.

Lasersko graviranje je lokalno „paljenje“ završnog transparentnog sloja strukture polimerne identifikacijske stranice pomoću laserske zrake čime se postiže kontrolirano i nepovratno zacrnjenje površine materijala. Upravo zbog toga je tehnika laserskog graviranja naišla na široku primjenu, jer je rezultat graviranja nemoguće izbrisati konvencionalnim metodama krivotvorenja.

Laserska zraka (lasera čvrstog stanja) kreće se po površini identifikacijske stranice te svakim svojim pulsom „pali“ jednu točkicu na polimernoj površini. Ovisno o trajanju pulsa, te faktorima frekvencije i primijenjene energije, laserski gravirana točkica će biti više ili manje zacrnjena. Lasersko graviranje nudi mogućnost dubinskog i taktilnog graviranja (slika). Dubinsko graviranje podrazumijeva graviranje u donjem dijelu završnog sloja, u dubini, bez destrukcije same površine, dok taktilno graviranje podrazumijeva graviranje duž cijele

vertikalne visine završnog sloja, a za posljedicu ima i uzdignutu površinu čime gravirani element postaje opipljiv.

Bilo da se radi o jednom ili drugom načinu ispisa, završni sloj (*overlay*) polimerne strukture mora biti transparentan te sadržavati specijalne aditive koji potiču paljenje i promjenu boje materijala.



Slika 37 - Skica taktilnog i dubinskog graviranja

Mogućnost taktilnog (opipljivog) i dubinskog graviranja pruža dodatno zaštitno svojstvo zbog kojeg je lasersko graviranje također zanimljivo.

Osim navedenoga, lasersko graviranje pruža mogućnost dva načina graviranja: vektorsko i rastersko graviranje (slika 38).

Slika 38 – Rastersko (lijevo) i vektorsko (desno) graviranje

Rasterskim graviranjem se ispisuju uglavnom slike, iako se može ispisivati i tekst, dok je vektorsko graviranje namijenjeno isključivo za ispis teksta. Vektorskim graviranjem najprije se ispisuje rub teksta neprekidnom linijom, a potom se ispunjava njegova površina. Prednost pred rasterskim graviranjem ima jer je za njega neophodno manje vremena. Rasterskim

graviranjem postiže se veliki broj gusto postavljenih točkica, slično kao i kod ink jet-a ili dot matrix printera. Iako ima prednost u postizanju visoke rezolucije, mana rasterskog graviranja je relativno dugo vrijeme ispisa u trajanju od cca. 10 sec. po jednoj slici putovnice standardne kvalitete kao i skupoće tehnologije.

8.4.1. Proizvodni koncepti izrade e-putovnica

U ovom poglavlju su prikazani osnovni proizvodni koncepti centraliziranog načina proizvodnje putovnica obzirom na korištenu tehniku personalizacije ali i tip putovnice okarakteriziran smještajem čipa i antene.

Centralizirani način izdavanja putovnica podrazumijeva izradu i personalizaciju putovnica u jednom, ovlaštenom proizvodnom pogonu države koje ispunjava visoke sigurnosne standarde fizičke i logičke zaštite.

U slučaju decentraliziranog načina izdavanja putovnica, *bianco* knjižice putovnice izrađene su u jednom proizvodnom pogonu, dok su procesi personalizacije izvođeni u većem broju državnih institucija, policijskih postaja ili općina. U ovakvom konceptu sustava izdavanja putovnica uvijek postoji opasnost od mogućih malverzacija *bianco* putovnicama koje su distribuirane na čitav niz različitih lokacija, koje najčešće ne pružaju dovoljno visoku razinu fizičke i logičke zaštite prostora i proizvoda. Decentralizirani način izdavanja putovnica najčešće je primijenjen u slučaju personalizacije putovnica u konzularnim predstavništvima države, radi skraćenja vremena isporuke putovnica u inozemstvu.

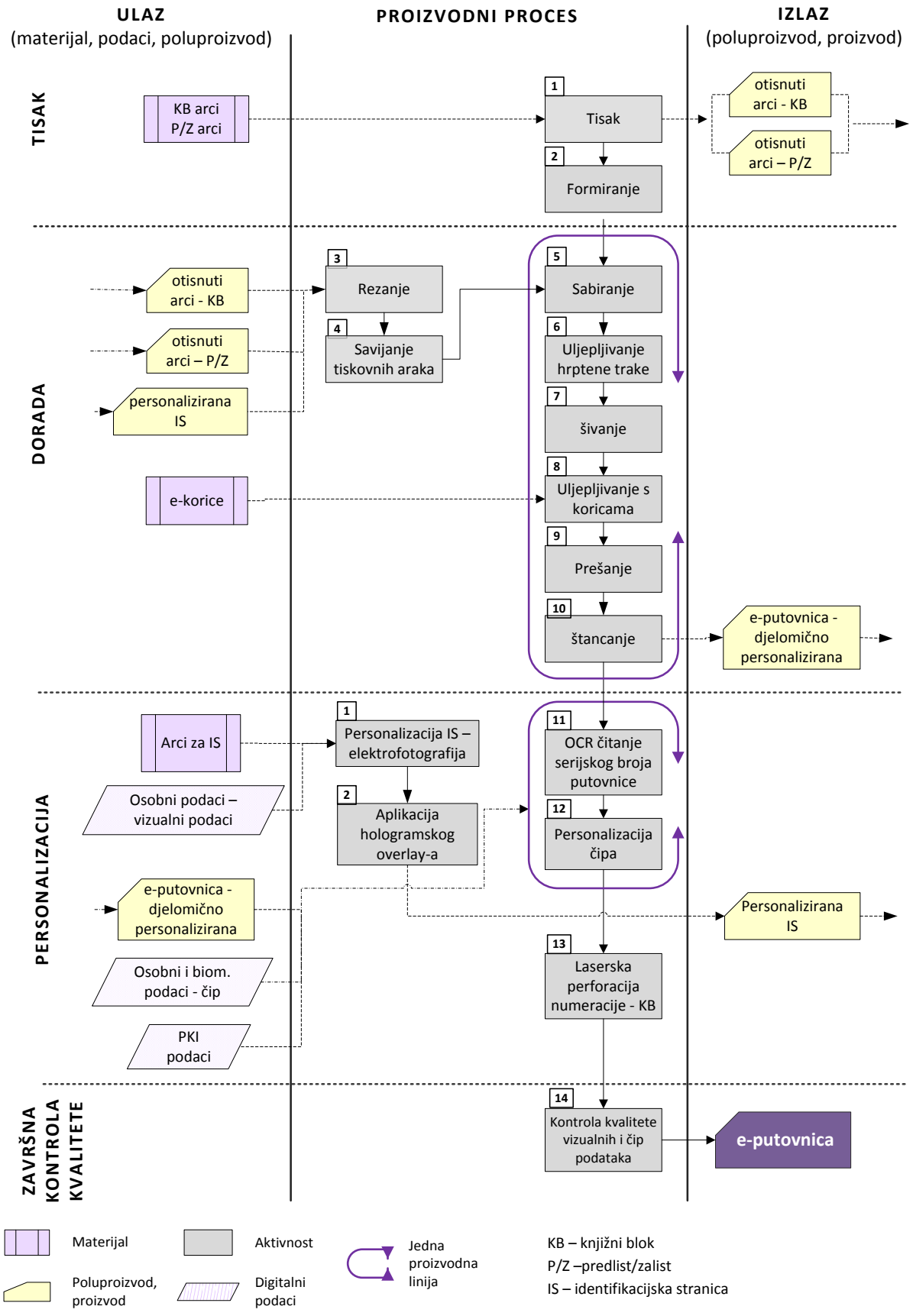
Jedna država može kombinirati i jedan i drugi način izdavanja putovnica, centralizirani za isporuku putovnica unutar matične države i de-centralizirani za isporuku putovnica u konzularnim predstavništvima.

U slučaju primjene isključivo centraliziranog načina izdavanja putovnica (kao što je to u Republici Hrvatskoj) neophodna je visoka logistička podrška i uhodan distribucijski lanac kako ne bi došlo do kašnjenja isporuka.

Ukupno je prikazano 6 osnovnih proizvodnih koncepata:

- Čip u koricama u kombinaciji s elektrofotografijom
- Čip u koricama u kombinaciji s ink jet-om
- Čip u koricama u kombinaciji s laserskim graviranjem
- Čip u polimernoj identifikacijskoj stranici u kombinaciji s laserskim graviranjem
- Čip u polimernoj *bianco* stranici u kombinaciji s elektrofotografijom
- Čip u polimernoj *bianco* stranici u kombinaciji s ink jet-om

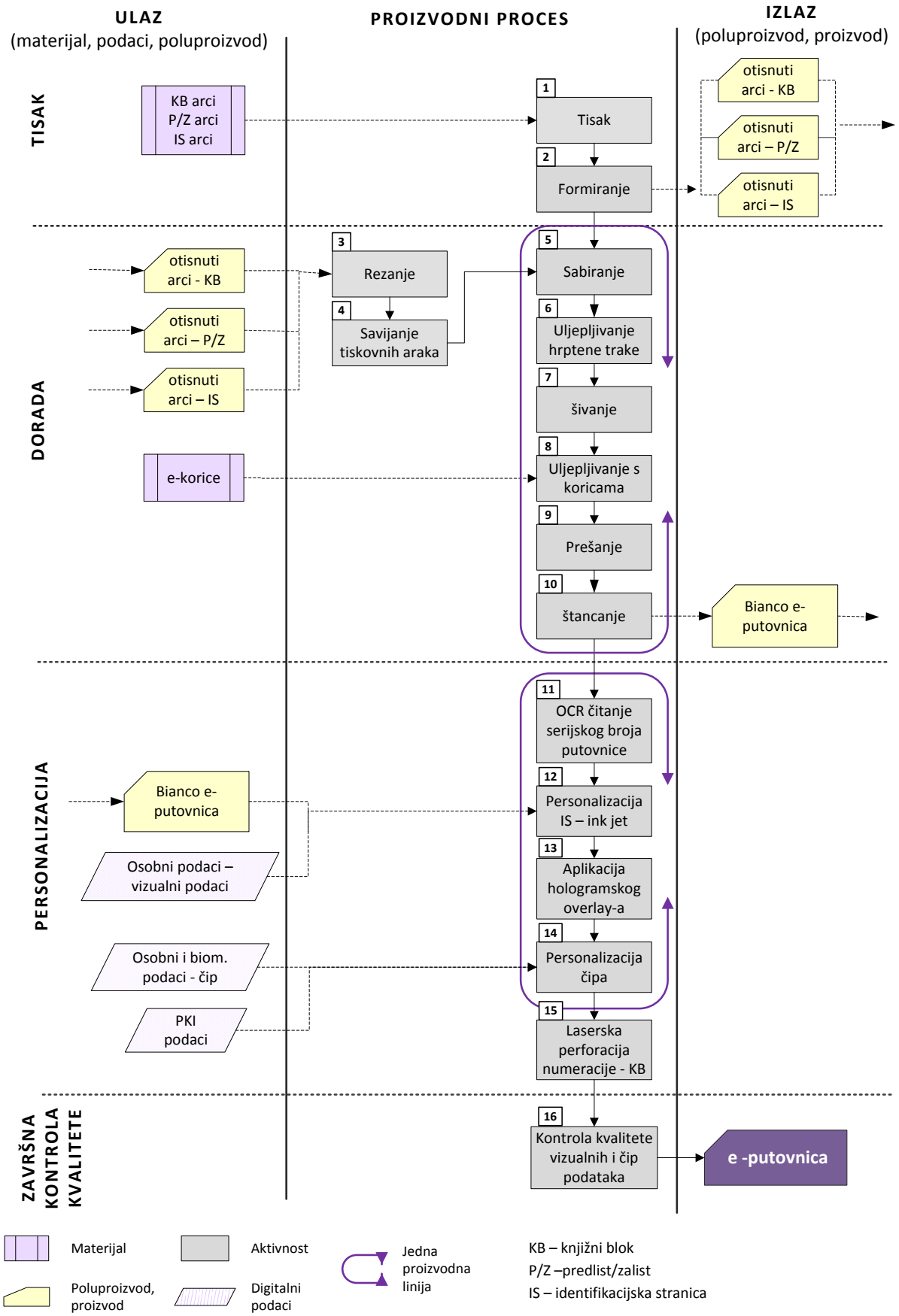
A) Čip u koricama u kombinaciji s elektrofotografijom



Dijagram 1 – Proizvodni tijek izrade putovnica sa e-koricama i personalizacijskom tehnikom elektrofotografije

Izradila: Željka Stražnicky, lipanj 2011.

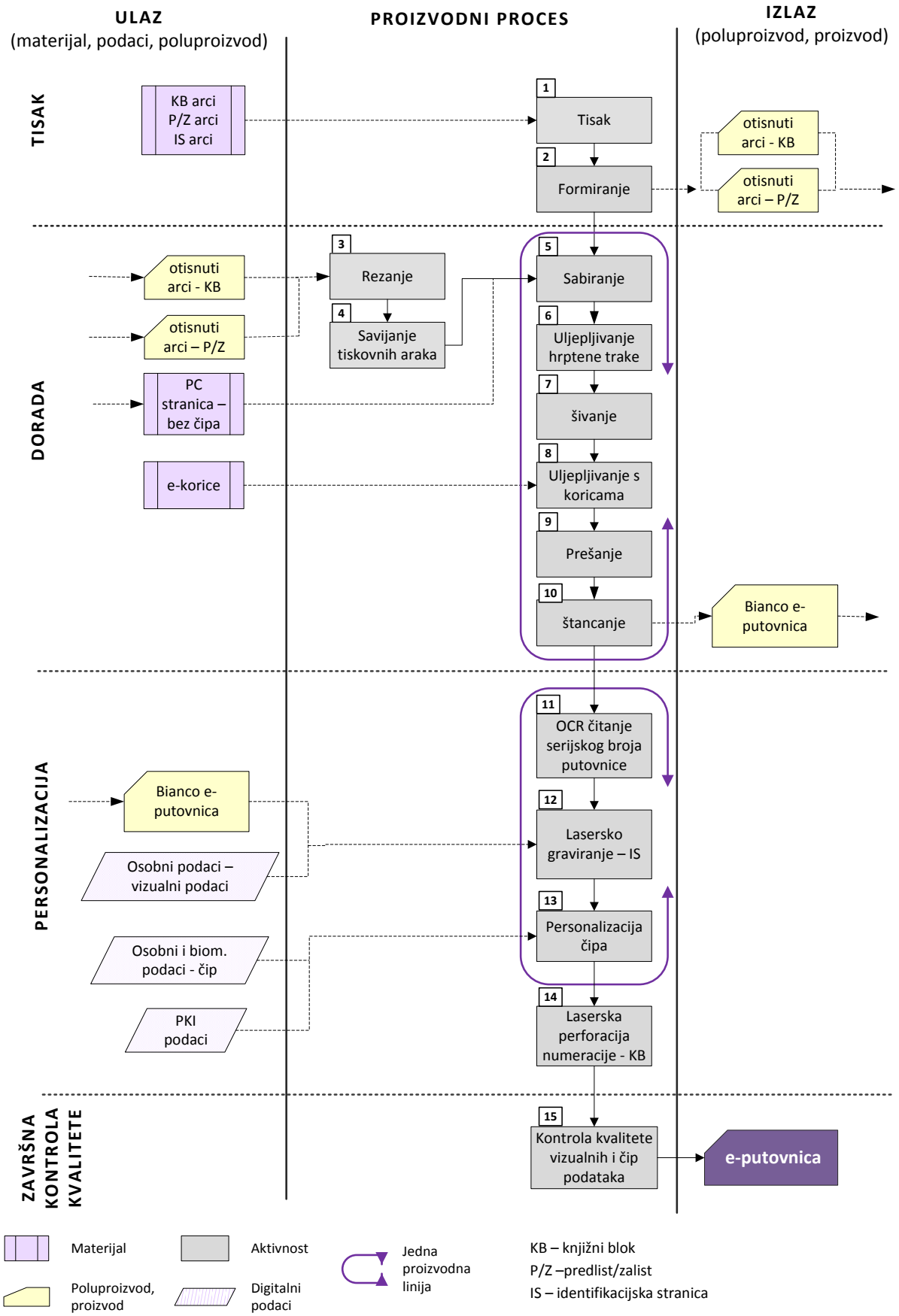
B) Čip u koricama u kombinaciji s ink jet-om



Dijagram 2 – Proizvodni tijek izrade putovnica sa e-koricama i personalizacijskom tehnikom ink jet-a

Izradila: Željka Stražnicky, lipanj 2011.

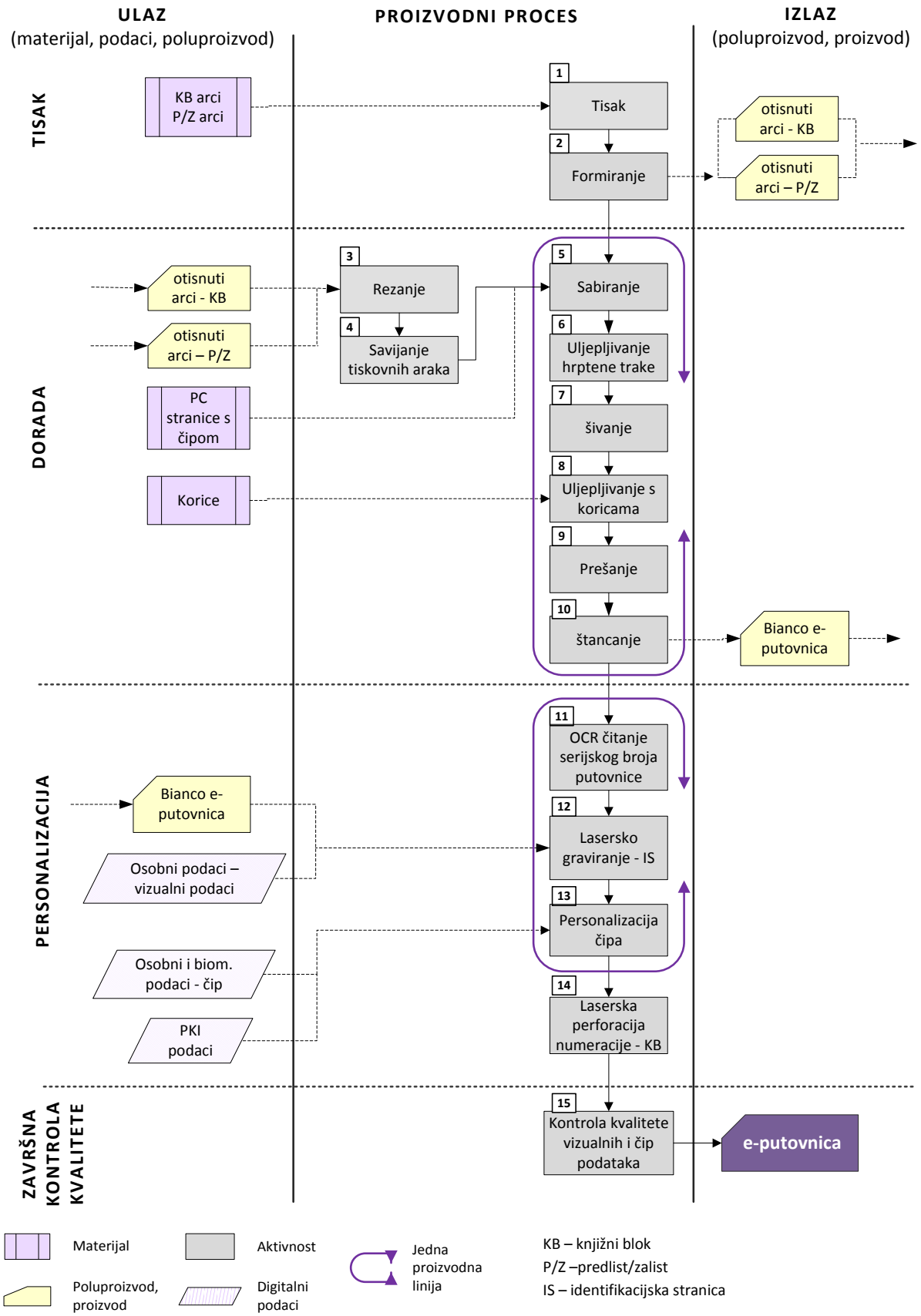
C) Čip u koricama u kombinaciji s laserskim graviranjem



Dijagram 3 – Proizvodni tijek izrade putovnica sa e-koricama i personalizacijskom tehnikom laserskog graviranja

Izradila: Željka Stražnicky, lipanj 2011.

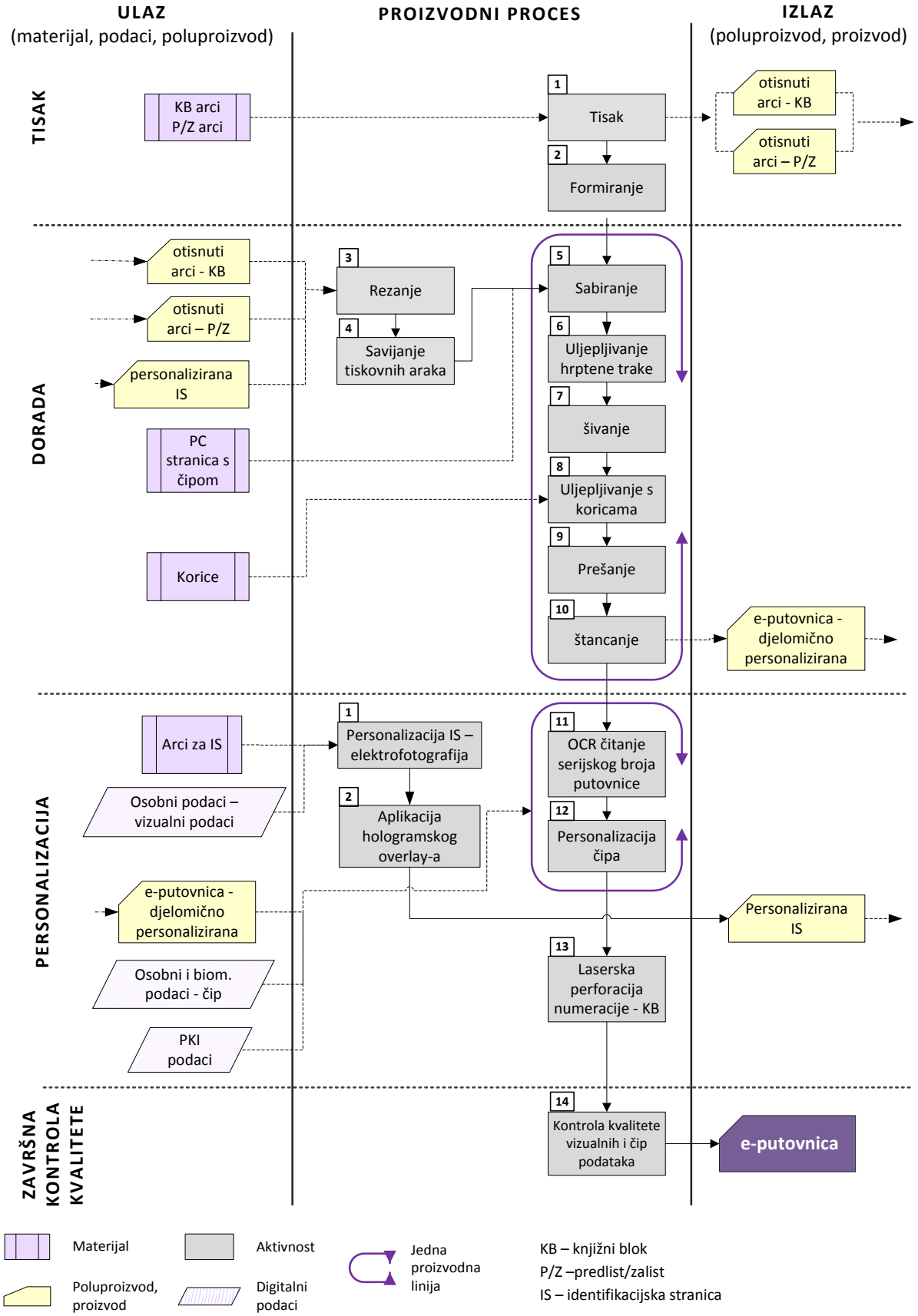
D) Čip u polimernoj identifikacijskoj stranici u kombinaciji s laserskim graviranjem



Dijagram 4 – Proizvodni tijek izrade putovnica sa PC stranicom i personalizacijskom tehnikom laserskog graviranja

Izradila: Željka Stražnicky, lipanj 2011.

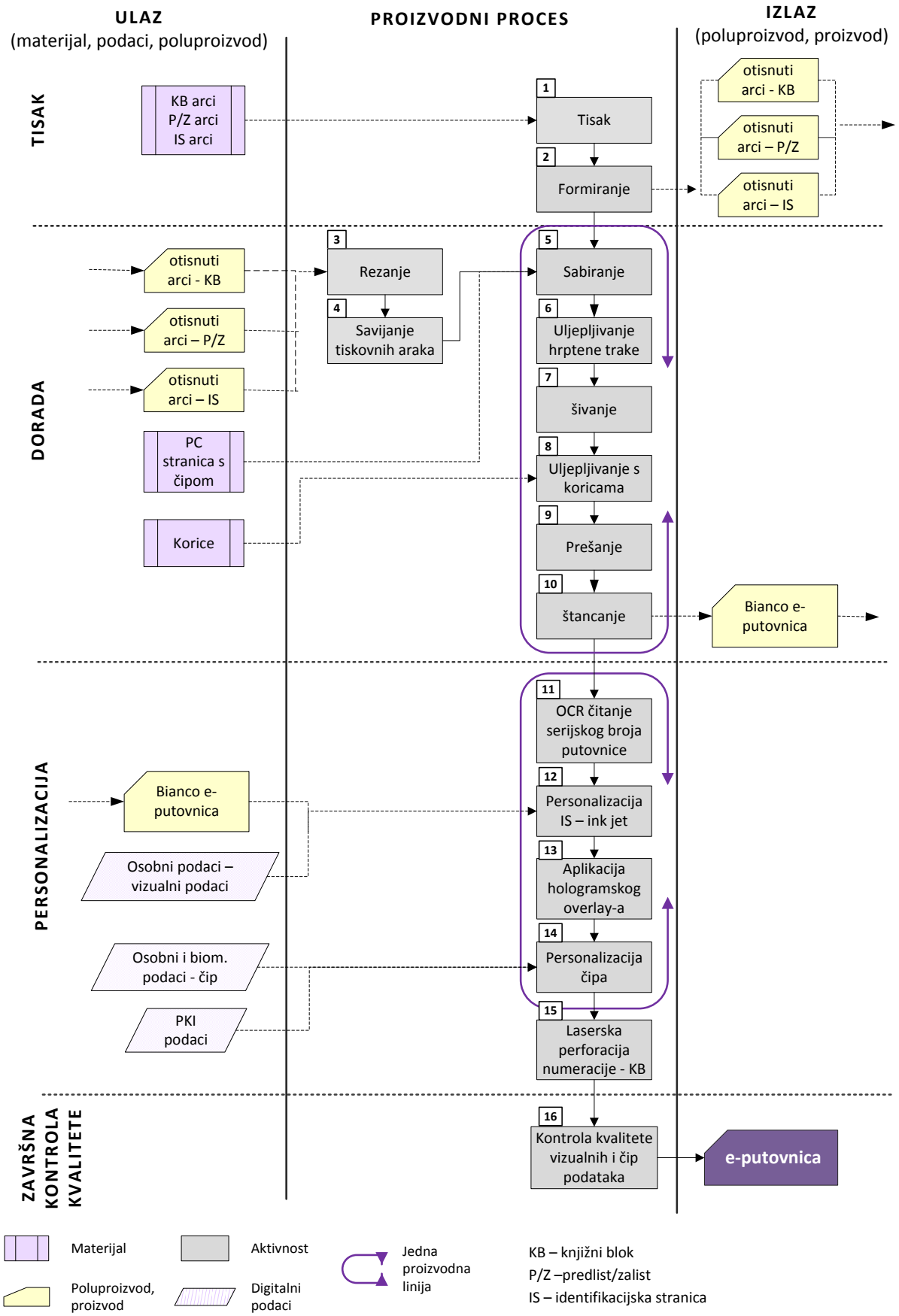
E) Čip u polimernoj *bianco* stranici u kombinaciji s elektrofotografijom



Dijagram 5 – Proizvodni tijek izrade putovnica sa PC bianco stranicom i personalizacijskom tehnikom elektrofotografije

Izradila: Željka Stražnicky, lipanj 2011.

F) Čip u polimernoj *bianco* stranici u kombinaciji s ink jet-om



Dijagram 6 – Proizvodni tijek izrade putovnica sa PC bianco stranicom i personalizacijskom tehnikom ink jet-a

Izradila: Željka Stražnicky, lipanj 2011.

Prednosti i nedostaci pojedinog proizvodnog koncepta navedeni su u slijedećoj tablici:

	Prednosti	Nedostaci
e-korice + elektrofotografija	✓ U slučaju postojanja tehnologije personalizacije u tvrtki, jednostavnija je tranzicija na dokument sa e-koricama. ✓ Financijski prihvatljivije rješenje u odnosu na ostale proizvodne koncepte.	✓ Personalizacija je sačinjena od 2 odvojena koraka: personalizacije IS stranice i e-korica. Greška u slučaju personalizacije korica podrazumijeva ponavljanje kompletnog procesa izrade knjižice putovnice uključujući i uvez. ✓ Nanašanje hologramskog overlay-a događa se u odvojenom koraku od personalizacije IS-e, što u slučaju pojave greške prilikom aplikacije podrazumijeva ponavljanje procesa personalizacije IS-a. ✓ E-korice su odvojene od IS-e čime se olakšava mogućnost krivotvorenja u smislu jednostavnije zamjene čipa bez implikacije po kvalitetu IS-e.
e-korice + ink-jet	✓ Stupanj automatizacije i linijskog načina rada na visokom nivou; personalizacija IS-e i čipa te nanašanje hologramskog overlay-a u istom prolazu kroz stroj. ✓ Mogućnost pohranjivanja *bianco* e-putovnica na zalihi, čime je proces maksimalno optimiziran proizvodni proces te skraćeno vrijeme isporuke proizvoda ✓ Financijski prihvatljivije rješenje u odnosu na ostale proizvodne koncepte.	✓ E-korice ne nudi dodanu vrijednost u smislu mogućnosti implementacije novih zaštitnih elemenata. ✓ Hologramski overlay nije ušiven u knjižni blok čime se povećava mogućnost krivotvorenja IS-e. ✓ E-korice su odvojene od IS-e čime se olakšava mogućnost krivotvorenja u smislu jednostavnije zamjene čipa bez implikacije po kvalitetu IS-e.
e-korice + lasersko graviranje	✓ Stupanj automatizacije i linijskog načina rada na visokom nivou; personalizacija IS-e i čipa u istom prolazu kroz stroj. Hologramski element integriran je u strukturu tanke polimerne stranice te je dio procesa proizvodnje IS-e, a ne personalizacije. ✓ Tanka polimerna stranica nudi dodanu vrijednost proizvodu u smislu mogućnosti implementacije niza novih zaštitnih elemenata. ✓ Mogućnost pohranjivanja *bianco* e-putovnica na zalihi, čime je proizvodni proces maksimalno optimiziran te skraćeno vrijeme isporuke proizvoda.	✓ E-korice su odvojene od IS-e čime se olakšava mogućnost krivotvorenja u smislu jednostavnije zamjene čipa bez implikacije po kvalitetu IS-e.
Čip u polimernoj IS + lasersko graviranje	✓ Stupanj automatizacije i linijskog načina rada na visokom nivou; personalizacija IS-e i čipa u istom prolazu kroz stroj. Hologramski element integriran je u strukturu polimerne stranice s čipom te je dio procesa proizvodnje IS-e, a ne personalizacije.	✓ Visoka cijena proizvodnje i personalizacije.

Izradila: Željka Stražnicky, lipanj 2011.

	✓ Polimerna stranica s čipom nudi dodanu vrijednost proizvodu u smislu mogućnosti implementacije niza novih zaštitnih elemenata. ✓ Mogućnost pohranjivanja *bianco* e-putovnica na zalihi, čime je proizvodni proces maksimalno optimiziran te skraćeno vrijeme isporuke proizvoda. ✓ Čip je integralni dio IS-e čime je otežana mogućnost zamjene čipa bez implikacije po cijelu IS-u te personalizirane vizualne podatke.	
Čip u polimernoj *bianco* stranici + elektrofotografija	✓ U slučaju postojanja tehnologije personalizacije u tvrtki, jednostavnija je tranzicija na dokument sa *bianco* polimernom stranicom.	✓ Visoka cijena proizvodnje i personalizacije koja nije opravdana dodanom vrijednošću proizvodu. ✓ Personalizacija je sačinjena od 2 odvojena koraka: personalizacije IS stranice i čipa *bianco* stranice. Greška u slučaju personalizacije čipa podrazumijeva ponavljanje kompletnog procesa izrade knjižice putovnice uključujući i uvez. ✓ *Bianco* polimerna stranica je odvojena od IS-e čime se olakšava mogućnost krivotvorenja u smislu jednostavnije zamjene čipa bez implikacije po kvalitetu IS-e. ✓ Iako *bianco* stranica sa čipom nudi mogućnost implementacije dodatnih zaštitnih elemenata, za navedeno ne postoji logično opravdanje jer *bianco* stranica ne sadrži personalizirane vizualne podatke koje je potrebno dodatno štititi.
Čip u polimernoj *bianco* stranici + ink jet	✓ U slučaju postojanja tehnologije personalizacije u tvrtki, jednostavnija je tranzicija na dokument sa *bianco* polimernom stranicom.	✓ Visoka cijena proizvodnje i personalizacije koja nije opravdana dodanom vrijednošću proizvodu. ✓ Personalizacija je sačinjena od 2 odvojena koraka: personalizacije IS stranice i čipa *bianco* stranice. Greška u slučaju personalizacije čipa podrazumijeva ponavljanje kompletnog procesa izrade knjižice putovnice uključujući i uvez. ✓ *Bianco* polimerna stranica je odvojena od IS-e čime se olakšava mogućnost krivotvorenja u smislu jednostavnije zamjene čipa bez implikacije po kvalitetu IS-e. ✓ Iako *bianco* stranica sa čipom nudi mogućnost implementacije dodatnih zaštitnih elemenata, za navedeno ne postoji logično opravdanje jer *bianco* stranica ne sadrži personalizirane vizualne podatke koje je potrebno dodatno štititi. ✓ Hologramski overlay nije ušiven u knjižni blok čime se povećava mogućnost krivotvorenja IS-e.

Tablica 17 - Popis prednosti i nedostataka proizvodnih koncepata izrade e-putovnica

Izradila: Željka Stražnicky, lipanj 2011.

9. BIOMETRIJA

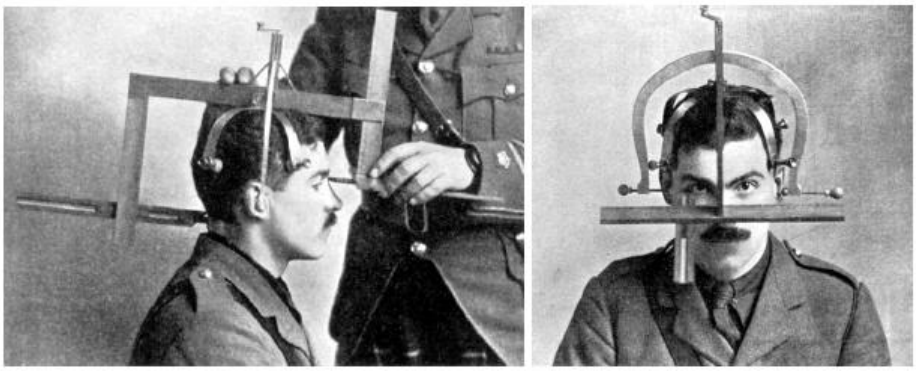
Pojam biometrije (grč. bios=život, metron=mjera) predstavlja znanost koja se bavi proučavanjem metoda za prepoznavanje ljudi, baziranih na jednome ili više jedinstvenih tjelesnih obilježja pojedinca. Drugačije rečeno, biometrija se koristi specifičnim fiziološkim i bihevioralnim karakteristikama osobe kako bi ju pozitivno prepoznala, tj. identificirala.

Biometrijska obilježja ljudi dijele se u 3 osnovne grupe:

- **Bihevioralna obilježja** (eng. *to behave* = ponašati se) – naučene aktivnosti koje osoba kroz život konstantno ponavlja. Odnose se na glas, potpis, dinamiku uporabe računalne tastature i dr.

- **Topološka obilježja** (grč. *topos* = mjesto) – fiziološke karakteristike koje su, uvjetno rečeno, konstantne kroz cijeli životni vijek pojedinca, a uključuju DNK zapis, geometriju lica, šarenicu oka, otisak prsta, geometriju ruke, vena, uha, usana i dr.

- **Diskretna (diskontinuirana) obilježja** – čine kombinaciju prethodno navedene dvije kategorije, a primjer je mrežnica oka (mrežnica oka mijenja svoje karakteristike ovisno o upadu svijetla na nju).



Slika 39 – Način mjerenja dimenzija glave čovjeka iz 1913. godine

Pri analizi i procjeni pojedinog biometrijskog obilježja, stručnjaci se vode značajkama poput jedinstvenosti, nepromjenjivosti, mogućnosti „prikupljanja“ obilježja, ergonomičnosti postupaka prikupljanja i dr., kako bi odredili primjenjivost obilježja u pojedinim postupcima identifikacije i autentifikacije. Jednostavnije rečeno, nije svako biometrijsko obilježje jednako pogodno za postupke identifikacije i autentifikacije u svakoj situaciji, to jest, neka su obilježja promatrana kroz navedene aspekte puno prihvatljivija od drugih. Na primjer, promatrano kroz aspekt jedinstvenosti i nepromjenjivosti, DNK zapis u ocjeni zauzima najviše mjesto, zbog čega je i temelj postupaka identifikacije u forenzičkim primjenama. No, izvan područja djelovanja forenzike, kod postupaka identifikacije i autentifikacije, npr. u sustavima davanja ovlasti pristupa određenim prostorijama i informacijama, ova se biometrijska osobina još uvijek ne primjenjuje. Razlog je prozaičan: U svim područjima poslovanja pa tako

i u primjeni biometrije, primarno mjesto zauzima profit. Naime, postupak „prikupljanja“ DNK zapisa i pretvaranja ovakvog zapisa u digitalno čitljivi oblik još uvijek je složen te zahtjeva skupi hardver koji zbog financijske nepristupačnosti ne bi naišao na široku primjenu. Nimalo zanemariva nije ni metoda prikupljanja DNK koja spada u kategoriju nametljivih. Postupci davanja krvi, sline ili drugog organskog dijela tijela čovjeka u komercijalne pa i državne svrhe, sigurno ne bi naišli na opće odobravanje i prihvaćanje od strane društva.

Zbog navedenoga, na listi najprihvatljivijih biometrijskih značajki u postupcima identifikacije nalaze se geometrija lica, otisak prsta te šarenica oka.

Konvencionalni postupci identifikacije ljudi odavna se provode pokazivanjem nečega što imamo, kao što je osobna iskaznica, putovnica ili neka dozvola. Ponekad se kod takvih postupaka također zahtjeva i nešto što znamo, poput zaporke ili PIN-a. No, kako tehnologija sve više i brže napreduje, a mogućnosti zlouporabe te iste tehnologije postaju također veće, javlja se potreba za korištenjem sigurnijih i pouzdanijih metoda i tada počinjemo koristiti nešto što jesmo: biometriju.

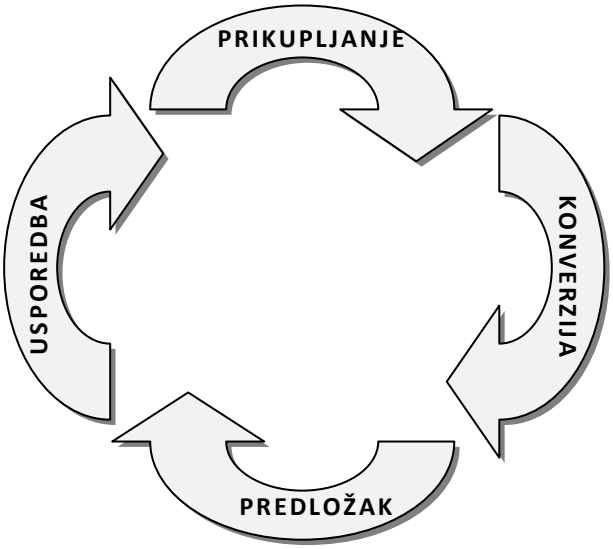
Nedostatak konvencionalne metode identifikacije, uporabom fizičkog identifikacijskog dokumenta, je u mogućnosti lažnog predstavljanja neke osobe ukoliko se domogne tuđeg dokumenta. Pa čak i ako taj dokument posjeduje fotografiju osobe, uz postojanje današnjih digitalnih tiskarskih tehnologija, ovakav oblik zaštite nije više nepremostiva prepreka. Glavna prednost biometrijskih metoda identifikacije je u tome što je biometrijska obilježja teško krivotvoriti, a njihovo postojanje zahtijeva da baš ta osoba koja se prepoznaje/identificira bude prisutna na mjestu identifikacije.

Da bismo mogli koristiti biometrijska obilježja za postupke identifikacije i autentifikacije potrebno je kreirati **biometrijski sustav**. Takav se sustav sastoji od skenera biometrijskih obilježja, softvera koji pretvara prikupljene informacije u digitalni oblik i baze podataka ili fizičkog medija u kojima se nalaze digitalno zapisani, prethodno prikupljeni, biometrijski podaci. Primjer jednog takvog jednostavnijeg sustava je autentifikacija za pristup računalu uz pomoć otiska prsta. Da bi takav sustav funkcionirao, potrebno je prethodno snimiti otisak prsta u za to predviđenu bazu podataka ili u neki fizički medij, kako bi se pri autentifikaciji mogla vršiti usporedba.

Stupanj sigurnosti biometrijskog sustava ovisi o samoj primjeni, tj. postoje različiti nivoi autentifikacije koji se u biometrijskom sustavu mogu primijeniti. Bez dobro kreiranog biometrijskog sustava sa strogo propisanim pravilima i protokolima rada, razina pouzdanosti i povjerenja u sustav pada, a mogućnost kompromitiranja sustava raste. Ovakav sustav autentifikacije i verifikacije omogućava visoki stupanj automatizacije i brzine rada, minimalni broj radnika i minimalni nivo birokracije, što je također jedan od glavnih razloga za njegovu sve veću i češću primjenu.

Glavne komponente biometrijskog sustava čine postupci:

- Prikupljanja „sirovih“ biometrijskih uzoraka.
- Ekstrakcije ili konverzije sirovog biometrijskog uzorka u među-oblik.
- Kreiranje predloška ili konverzija među-oblika u biometrijski predložak pogodan za digitalnu pohranu.
- Usporedbe novog prikupljenog biometrijskog uzorka sa pohranjenim referentnim biometrijskim predloškom.



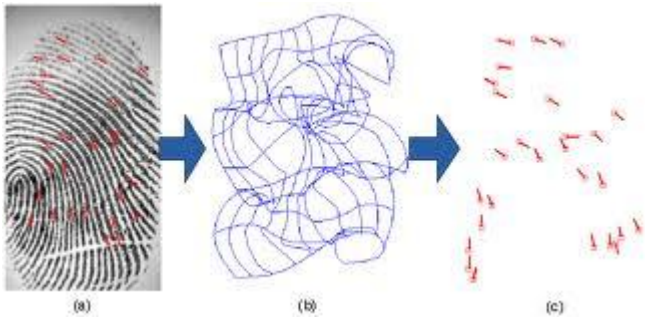
Slika 42 – Skica tijeka osnovnih procesa biometrijskog sustava provjere

Postupak prikupljanja „sirovih“ biometrijskih uzoraka događa se kod osoba koje, primjerice, apliciraju za izdavanje elektroničke putovnice. Postupak prikupljanja „sirovog“ biometrijskog uzorka i njegovo pretvaranje u biometrijski predložak je proces za koji je neophodan uređaj poput skenera otisaka prstiju, skenera fotografija, digitalne kamere za snimanje slike „uživo“ ili kamere za snimanje šarenice oka. Svaki od uređaja za prikupljanje biometrijskog uzorka zahtjeva postojanje određenih kriterija i definiranih procedura koje je potrebno poštivati kako bi se postigla zadovoljavajuća kvaliteta uzorka.

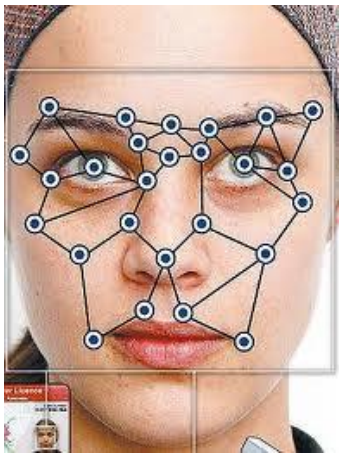
Slika 40 – Postupak „uzimanja“ otiska jednog ili više prstiju

Slika 41 – Postupak „uzimanja“ digitalne slike lice (desno); postupak „uzimanja“ šarenice oka (lijevo)

Postupak kreiranja biometrijskog predloška podrazumijeva očuvanje izrazitih i ponovljivih biometrijskih elemenata iz uzetog/snimljenog biometrijskog uzorka, a događa se uz pomoć softverskog algoritma koji je vlasničko rješenje proizvođača specifičnog uređaja za prikupljanje biometrije. Takvom softverskom algoritmu svojstvena je i kontrola kvalitete uzorka koja je dijelom ugrađenih i definiranih mehanizama provjere. Budući da su sve biometrijske provjere i usporedbe ovisne o kvaliteti originalnog uzorka, postavljeni standardi kvalitete moraju biti što viši. Ukoliko pred-definirana razina kvalitete nije postignuta, postupak uzimanja biometrijskog uzorka mora se ponoviti.



Slika 42 – Postupak pretvaranja biometrijskog uzorka (a) u biometrijski predložak (c)



Slika 43 – Primjer karakterističnih elemenata biometrijskog uzorka lica koji čine temelj za stvaranje biometrijskog predloška

9.1. Biometrija u e-putovnicama

Nakon nekoliko godina istraživanja pogodnosti primjene različitih biometrijskih identifikatora, ICAO je zaključio kako je geometrija lica najpogodniji oblik za globalnu interoperabilnu biometrijsku verifikaciju na graničnim prijelazima. Također, pored geometrije lica, opcionalno se koriste i 2 otiska prsta (a u EU obavezno) i šarenica.

Prednosti koje ICAO veže uz primarni biometrijski identifikator su [10]:

- fotografija lica je informacija koju osobe i inače izlažu javnosti,
- fotografija lica je kulturološki prihvaćena u međunarodnim razmjerima,
- fotografija lica je podatak koji se godinama prikuplja i verificira u postupcima zaprimanja zahtjeva za izradu putovnica,
- javnost je upoznata sa mogućnosti snimanja lica i uporabe za postupke verifikacije,
- snimanje lica nije nametljiva metoda, što znači da osoba ne mora imati bilo kakav oblik fizičke interakcije s uređajem koji vrši snimanje,
- snimanje lica ne zahtjeva nove i skupe procedure snimanja,
- postupci snimanja lica se mogu primijeniti u kratkom roku,
- mnoge države su već imale baze podataka digitaliziranih fotografija osoba koje su aplicirale za izdavanje putovnica,
- generalno gledajući fotografije lica su jedina biometrija dostupna u širim razmjerima za identifikaciju, npr. u slučaju tjeralica,
- postupak verifikacije osobe na osnovu slike lice od strane službenika je relativno jednostavan i uobičajen proces na graničnim prijelazima.

Usporedna analiza prednosti i nedostataka uporabe 3 tipa biometrije predložene od strane ICAO-a prikazane su u tablici:

	Slika lica	Otisak prsta	Slika šarenice
prednosti	Prihvaćeno od javnosti Lagano za uporabu Korištenje u „tjeralicama“	Zrela tehnologija Visoka točnost verifikacije Otisci su stabilni kroz vrijeme	Visoka točnost verifikacije Slika šarenice je stabilna kroz vrijeme
nedostaci	Upitna točnost verifikacije Pitanja vezana uz starenje kroz vrijeme	Niska prihvatljivost od javnosti	Nova tehnologija Nametljiva metoda Malo proizvođača

Tablica 18 - Popis prednosti i nedostataka biometrijskih identifikatora slike lica, otiska prsta te šarenice

Osnovna smisao postojanja biometrijskih identifikatora u putovnici je mogućnost verifikacije identiteta osobe i putovnice s kojom se predstavlja. Nekoliko je mogućih primjena biometrije u procesima zaprimanja zahtjeva za izradu putovnice i u procesima provjere na graničnim prijelazima.

Tijekom snimanja biometrijske slike lica ili otisaka prstiju u procesu apliciranja osobe za izdavanje putovnice, netom uzeta slika može se provjeriti sa postojećom biometrijskom bazom u nadležnosti države (ukoliko postoji), kako bi se eventualno utvrdilo da li je osoba koja aplicira za izdavanje putovnice već otprije poznata nekom od postojećih sustava (npr. da li ima kriminalni dosje, da li već posjeduje putovnicu neke druge države i sl.).

Kada osoba koja je aplicirala za izdavanje putovnice podiže putovnicu po njenoj izradi, biometrijska slika lica ili otisaka prstiju može biti ponovno uzeta kako bi se verificirala s prvotno uzetim podacima. Također, može biti provjeravan i identitet osoblja koje učestvuje u procesu zaprimanja zahtjeva za izdavanje putovnica na način da se biometrijski autentificira u sustavu, kako bi dobila dozvolu za nastavak rada.

U postupcima provjere e-putovnica na graničnim prijelazima postoji nekoliko mogućih scenarija provjere. Dvostruka provjera podrazumijeva provjeru netom uzete slike nositelja putovnice na graničnim prijelazima sa slikom spremljenom u čip putovnica (ili u centralnoj bazi podataka), kako bi se utvrdilo da putovnica nije mijenjana. Trostruka provjera značila bi provjeru netom uzete slike nositelja putovnice sa slikom spremljenim u čip te sa slikom spremljenom u centralnu bazu podataka. Dok četverostruka provjera podrazumijeva vizualnu provjeru svih slika iz trostruke provjere sa otisnutom slikom u putovnici.

Efikasnost biometrijskih sigurnosnih sustava opisana je pomoću dva osnovna tipa grešaka:

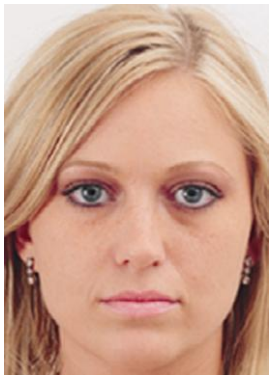
- **FAR** (engl. False Acceptance Rate) – omjer prihvaćenih lažnih uzoraka i ukupnog broja odbačenih uzoraka
- **FRR** (engl. False Rejection Rate) – omjer odbačenih ispravnih uzoraka i ukupnog broja odbačenih uzoraka

Cilj kvalitetnog sustava prepoznavanja je postići što nižu vrijednost za FAR i FRR. Jedan od načina smanjenja postotka ovih grešaka je korištenje multi-modalnih biometrijskih sustava koji kombiniraju provjeru identiteta pomoću više od jedne biometrijske značajke osobe.

Zahtjevi vezani uz biometrijske podatke u e-putovnici

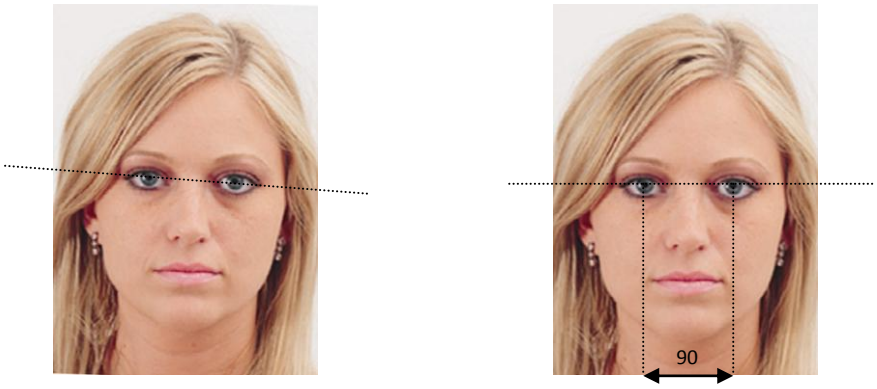
Najveći udio u zauzetom prostoru unutar LDS aplikacije (ili u memoriji čipa) nosi slika. Zbog toga se slika mora komprimirati kako bi zauzimala što manje prostora ali na način da ne ugrozi potrebnu kvalitetu neophodnu za biometrijsku verifikaciju. Za kompresiju slike koriste se JPEG i JPEG2000 algoritmi, pa se u konačnici komprimirana veličina slike kreće u rasponu od 15 – 20 Kb.

Kako bi prepoznavanje osobe bilo olakšano, ICAO je propisao i neka dodatna pravila za pohranjivanje slike u čip koja su usklađena sa specifikacijama ISO/IEC 19794-5. Slika koja se nalazi u čipu mora biti identična slici koja je personalizirana na identifikacijskoj stranici. Minimalno može biti skraćena tako da obuhvaća vrh brade i vrh glave kao na slici 44.



Slika 44 - Maksimalno skraćena slika (izvor: AKD)

Slika mora biti spremljena ili kao potpuno frontalna slika lica ili kao „*token*“ slika (token, eng. dokaz). “*Token*“ slika je ona slika kod koje je izvršena rotacija (ukoliko je potrebno) koja osigurava da je zamišljena horizontalna linija koja prolazi kroz centar očiju osobe u potpunosti paralelna sa gornjim rubom slike. Također, kod “*token*“ slike lica udaljenost među centralnim točkama očiju je cca. 90 piksela kao na slici 45. Kako bi se zadovoljio zahtjev od 90 piksela među očima, originalna slika uglavnom mora biti re-semplirana.



Slika 45 – Originalna slika (lijevo) i „Token“ slika (desno) (izvor: AKD)

Kada se govori o otisku prsta optimalna veličina u komprimiranom stanju kreće se oko 10 K po prstu. Preporuka za formatom kompresije je WSQ (*Wavelet Scalar Quantization*) tehnika. Ukoliko se radi o slici šarenice tada je optimalna veličina slike oko 30 K po šarenici (prema specifikacijama ISO/IEC 19794-6).

Sumirani prikaz biometrijskih podataka, njihovih formata i preporučenih veličina dan je u tablici:

BIOMETRIJSKI PODATAK	FORMAT	VELIČINA
SLIKA LICA	JPEG, JPEG 2000	15 – 20 K
OTISAK PRSTA	WSQ	10 K (1 prst)
SLIKA ŠARENICE (IRISA)	WSQ	30 K (po oku)

Tablica 19 - Popis formata i veličina biometrijskih identifikatora slike lica, otiska prsta te šarenice za uporabu u e-putovnicama

Iako je konačna veličina memorije beskontaktnog čipa e-putovnice izbor pojedine države, ICAO daje preporuku na uporabu minimalno 32 K EEPROM memorije (***E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory* – elektronički izbrisiva sa mogućnošću programiranja memorija sa mogućnošću čitanja). Kada se analiziraju podaci koje je neophodno pohraniti u čip: slika lica, podaci strojno čitljive zone, podaci vezani uz sigurnost – certifikati, ključevi i sl., uz pohranu opcionalnih podataka (u EU obaveznih) - otisaka prstiju, tada se dolazi do zaključka kako potrebna veličina memorije prelazi minimalnu preporuku od 32 K.

Također, za optimalno funkcioniranje čipa te komunikaciju sa terminalima nije preporučljivo kompletnu dostupnu memoriju „napuniti“ podacima. Stoga su na tržištu najčešće korištene memorije čipa od 64 K, 72 K i 80 K EEPROM memorije.

Postupci prikupljanja biometrijskih podataka

Prikupljanje biometrijskih podataka događa se u postupcima predaje zahtjeva za izradom putovnica. Mjesta za prikupljanje zahtjeva za izradom putovnica najčešće su policijske postaje, općine ili neke druge slične državne institucije.

Sustavi prikupljanja biometrijskih i drugih demografskih podataka neophodnih za izradu putovnica mogu se podijeliti na:

- „*live capturing*“ sustave (sustavi za prikupljanje podataka u digitalnom obliku)
- Konvencionalne sustave
- Kombinaciju „*live capturing*“ i konvencionalnih sustava

„*Live capturing*“ sustavi prikupljanja podataka predstavljaju sustave u kojima se podacima u samom startu prikupljaju u digitalnom obliku korištenjem uređaja poput digitalnih kamera, skenera otisaka prstiju, skenera šarenica i potpisnih digitalnih podložaka (eng. *signature pad*). Takvim sustavom upravlja specijalizirana softverska aplikacija koja automatski korigira prikupljene podatke u oblik sukladan ICAO zahtjevima. I unutar „*live capturing*“ sustava postoje varijacije koje se uglavnom odnose na oblik integracije različitih digitalnih uređaja te zahtijevani način i mjesto uporabe. Nekoliko je primjera takvih sustava prikazanih na slikama 46, 47, 48 i 49.

Slika 46 - Desktop sustav za prikupljanje podataka

Slika 47 – Mobilni kovčeg za prikupljanje podataka

Slika 48 – „Toranj“ za prikupljanje podataka

Slika 49 – Kabina za prikupljanje podataka

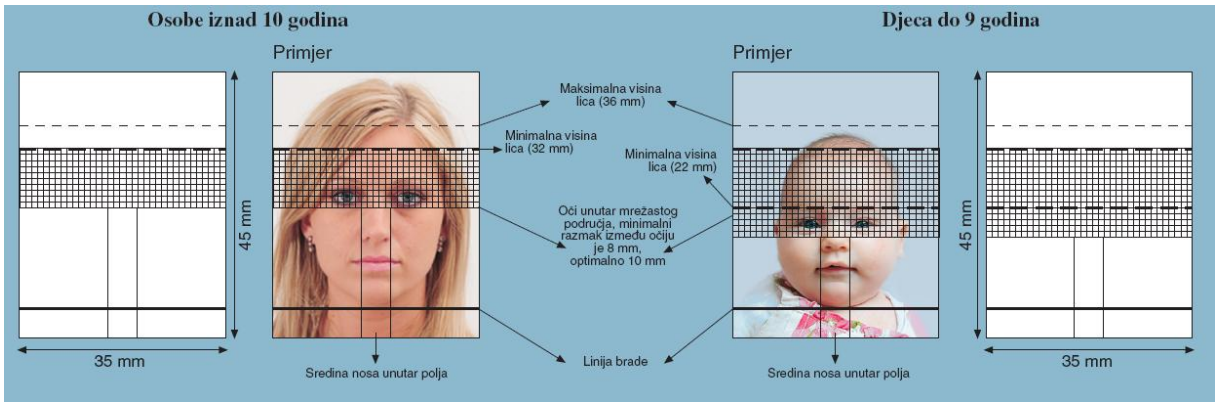
Konvencionalni sustavi prikupljanja podataka podrazumijevaju ručni upis podataka u papirnate obrasce za izdavanje putovnica te prilaganje konvencionalne fotografije od strane osoba koje apliciraju za izdavanje putovnica. Službenik predani zahtjev potom unosi u odgovarajuću aplikaciju u računalo te skenira priloženu fotografiju.

Slika 50 – Skener obrasca sa ulijepljenom fotografijom

Kako „*live capturing*“ sustavi predstavljaju veliki financijski izdatak za države koje kreću u izdavanje e-putovnica, tako većina država zadržava postojeće konvencionalne metode prikupljanja podataka, a unaprjeđuju softverske aplikacije koje obrađuju prikupljene podatke kako bi ih spremile u odgovarajućoj kvaliteti. Ovakav konvencionalni sustav moguće je u potpunosti zadržati kod implementacije e-putovnica 1. generacije, dok je kod implementacije e-putovnica 2. generacije potrebno integrirati i skenere otisaka prstiju i tada je takav sustav kombinacija konvencionalnog i „*live capturing*“ sustava.

Bilo da se radi o konvencionalnom sustavu ili kombinaciji konvencionalnog i „*live capturing*“ sustava, određene je mjere, za provjeru prikladnosti fotografija biometrijskim zahtjevima, potrebno implementirati. Budući da se fotografije skeniraju sa fizičkog medija u digitalni, neophodno je da fotografi primjenjuju određene zakonitosti kako bi konačna prilagodba kvalitete u policijskim postajama mogla biti provedena na odgovarajući način. U takvim su situacijama neophodne adekvatne edukacije fotografa te primjena alata za provjeru sukladnosti fotografija.

Jedan od takvih alata je i jednostavna šablona otisnuta na prozirnoj podlozi koja se prislanja na fotografiju i kojom se provjerava sukladnost fotografije u fotografskim radnjama i policijskim postajama (slika 51).



Slika 51 – Šablona za provjeru sukladnosti fotografija (izvor: AKD)

Iako financijski ne-prihvatljiviji, „*live capturing*“ sustavi nude nekoliko prednosti nad ostala dva jer omogućuju potpuno automatizirani postupak prikupljanja podataka bez postojanja među-koraka koji uključuje rad policijskih službenika, te postizanje kvalitete biometrijskih podataka zbog ne-postojanja konvencionalnih metoda razvijanja fotografije te skeniranja u digitalni oblik čime je nemoguće u potpunosti izbjeći određeni stupanj degradacije.

10. PKI INFRASTRUKTURA

10.1. Uvod u PKI infrastrukturu

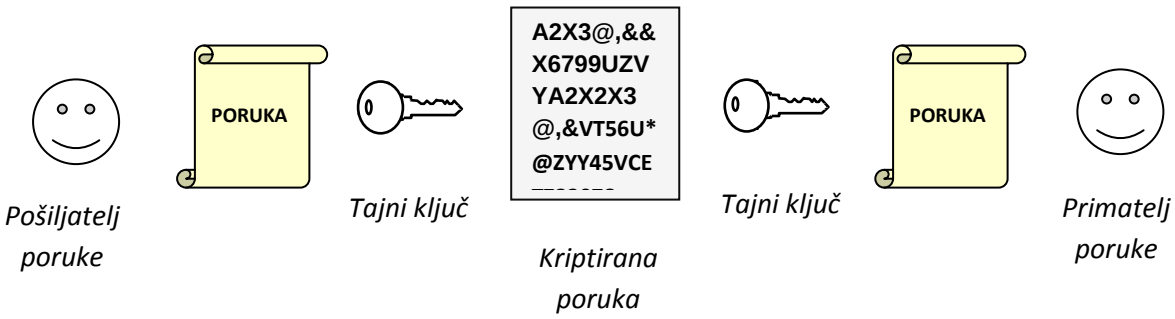
PKI infrastruktura (PKI – *Public Key Infrastructure*) ili infrastruktura javnih ključeva je skup hardvera i softvera, politika i procedura kojima se opisuje način kreiranja, upravljanja, distribucije, uporabe, pohranjivanja i povlačenja digitalnih certifikata. Temelji se na principu asimetrične kriptografije, tj. zaštite uporabom 2 različita ključa.

Središnjicu sustava izdavanja, uporabe i provjere e-putovnica čini upravo infrastruktura javnih ključeva kao najviši oblik koncepta zaštite podataka koji danas postoji. Sigurnosni mehanizmi ovog oblika infrastrukture primarno osiguravaju autentičnost, integritet, povjerljivost i neporecivost podataka pohranjenih u čipu putovnice.

Razlog prvotnog razvoja PKI infrastrukture prvenstveno je ležao u potrebi rješavanja velikih sigurnosnih pitanja i pitanja integriteta podataka kao posljedice sve više rastućeg interneta te e-trgovanja krajem prošlog stoljeća. Danas, infrastruktura čini temelj svih onih sustava koji žele osigurati visoki stupanj vjerodostojnosti i povjerenja, sa širokim spektrom primjene kako u internetskom poslovanju, tako i u raznim identifikacijskim sustavima.

Osnova PKI infrastrukture leži u kriptografskim procesima enkripcije i dekripcije podataka. Enkripcija i dekripcija podataka bazira se na matematičkim funkcijama, odnosno algoritmima, kojima se bitovi jasnog teksta pretvaraju u bitove kriptiranog teksta i obratno.

U postupcima enkripcije i dekripcije podataka razlikuju se simetrična i asimetrična kriptografija. Simetrična kriptografija je stariji oblik kriptografije koji koristi jedan (isti) ključ i za enkripciju i dekripciju podatka, uporabom algoritma DES i 3DES (*Data Encription Standard* razvijen 1975.god. [12]).

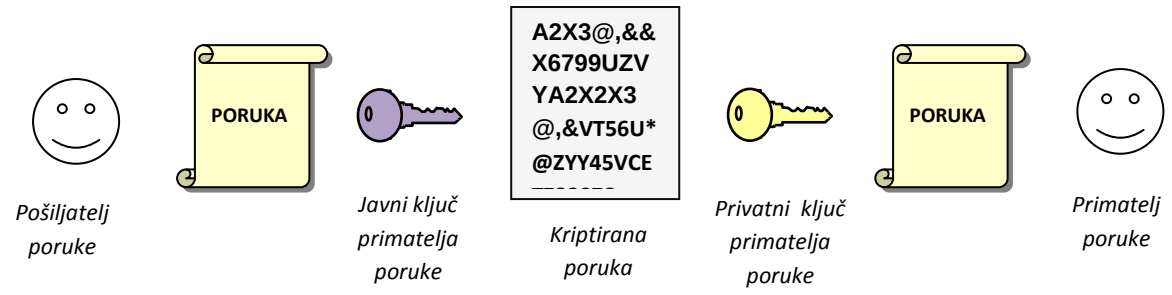


Slika 52 - Princip simetrične kriptografije

Najveći problem asimetrične kriptografije leži u razmjeni tajnog ključa između pošiljatelja i primatelja odnosno u povjerljivosti kanala za razmjenu, u kojem je potrebno osigurati njegovu zaštitu te smanjiti mogućnost krađe.

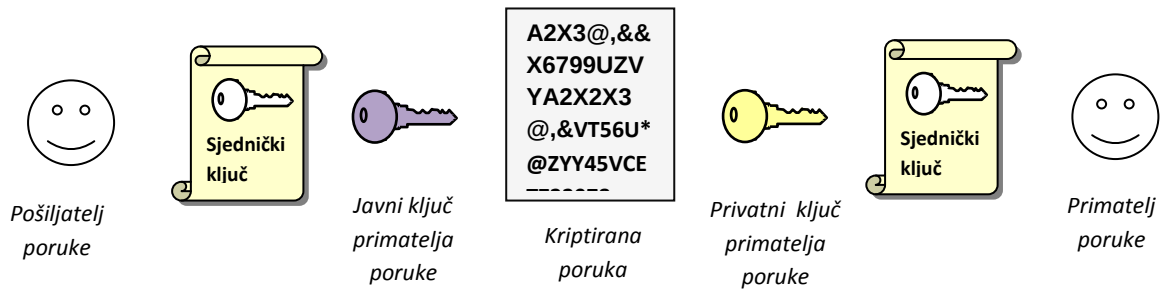
Mnogo robusnija i sigurnija enkripcijska tehnologija leži na principu asimetrične kriptografije na kojoj je i bazirana infrastruktura javnih ključeva. Asimetrična kriptografija temelji se na postojanju 2 para ključeva, javnom i tajnom ključu.
Princip asimetrične kriptografije predstavili su Whitfield Diffie and Martin Hellman, 1976. god. u svom radu “*New Directions in Cryptography”.*

Javni ključ je dostupan javnosti, on je objavljen, a služi za kriptiranje poruke. Tajni ključ je poznat samo vlasniku ključa te se on koristi za dekriptiranje poruke. Time se kriptiranje poruka između dvije strane (primatelja i pošiljatelja) može izvesti bez otkrivanja/dijeljenja privatnog ključa. Sigurna razmjena poruka asimetričnim kriptiranjem teče na način da pošiljatelj kriptira svoju poruku sa javnim ključem primatelja, a primatelj dekriptira poruku uporabom svog privatnog ključa koji je samo njemu poznat. Ovaj proces kriptiranja najprije podrazumijeva razmjenu javnih ključeva između dvije strane. Komunikacijski kanal za razmjenu nije ugroza za ključ budući da sigurnost ovog mehanizma leži u nemogućnosti dobivanja/izračunavanja privatnog ključa na temelju poznavanja javnog ključa. Stoga je javne ključeve moguće razmijeniti npr. putem elektroničke pošte. Međutim, ukoliko se govori o razmjeni nešto osjetljivijih podataka, poput broja kreditnih kartica i sl., tada se primjenjuju sofisticiraniji mehanizmi bazirani na asimetričnom kriptiranju.



Slika 53 - Princip asimetrične kriptografije

Algoritam kojeg koristi asimetrična kriptografija je RSA (*Rivest, Shamir, Adleman*). RSA algoritmima nije moguće kriptirati velike količine podataka, jer bi postupak dekriptiranja trajao jako dugo. Zbog toga se asimetrična kriptografija koristi za razmjenu tzv. sjedničkih ključeva kojima se kriptira sjednica odnosno komunikacija između dva subjekta. Sjednički ključevi su bazirani na simetričnoj kriptografiji koja može kriptirati veće količine podataka.
Valjanost sjedničkih ključeva je vrlo kratka radi sigurnosnih razloga, obično onoliko koliko traje jedna sjednica, odnosno komunikacija između dva subjekta. Trajanje para ključeva asimetrične kriptografije traje znatno duže i nije ga potrebno često mijenjati.



Slika 54 - Razmjena sjedničkih ključeva uporabom asimetrične kriptografije

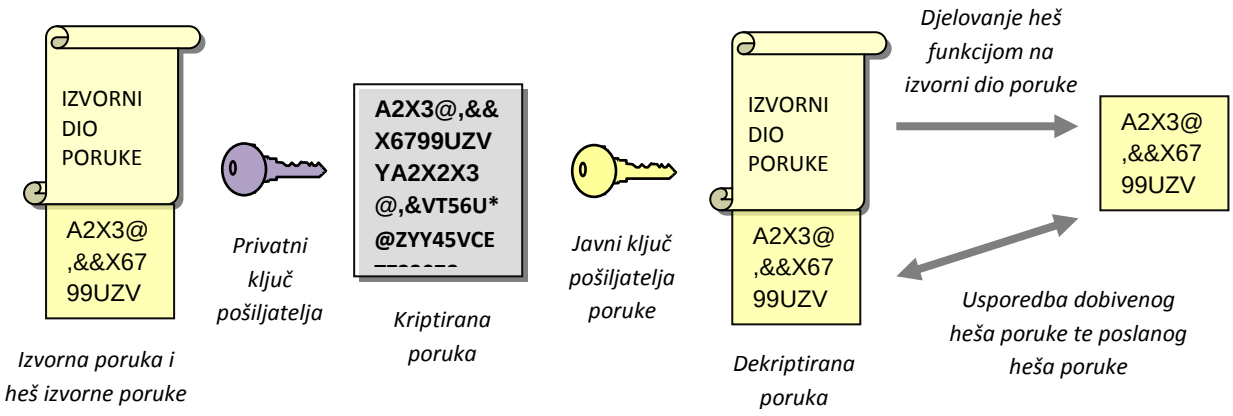
Svojstvo pojedinih algoritama asimetrične kriptografije je također i slijedeće: ukoliko se neki podatak šifrira privatnim ključem moguće ga je dešifrirati jedino odgovarajućim javnim ključem, a u slučaju da je podatak šifriran javnim ključem tada ga je moguće dešifrirati isključivo pripadajućim privatnim ključem. Ovo ključno svojstvo omogućava digitalno potpisivanje dokumenata ili digitalni potpis, kao temeljni element PKI infrastrukture.

10.2. Digitalni potpis

Digitalni potpis predstavlja matematičku funkciju – tehnike heša kojima se djeluje na podatak ili poruku koja se želi potpisati i poslati. Digitalni potpis potvrđuje integritet i autentičnost poruke i pošiljatelja jer je samo njemu poznata heš funkcija kojom je digitalni potpis kreiran.

Heš funkcijom se djeluje na bitove podataka, a rezultat je broj ili niz bitova koji se zovu rezultat pregleda poruke (message digest). Dobiveni rezultat ne predstavlja kriptiranu poruku već proizvoljan matematički rezultat sličan onome koji se dobije postupkom izračuna kontrolnih oznaka strojno čitljive zone putovnice.

Heš funkcija prethodi procesu kriptiranja, pa jednom kada je ona provedena nad porukom koristi se privatni ključ pošiljatelja za enkripciju poruke. Ovaj ključ nije poznat nikome drugome osim pošiljatelju pa se smatra vrlo sigurnim ključem. Poruka prije procesa kriptiranja sadrži izvorni dio poruke i heš dio poruke. Primatelj može dekriptirati poruku uporabom odgovarajućeg javnog ključa, a ponavljanjem heš funkcije na izvorni dio poruke i usporedbom sa dobivenim hešom verificira autentičnost.



Slika 55 – Proces digitalnog potpisa

Izradila: Željka Stražnicky, lipanj 2011.

Digitalni potpis zamjenjuje funkciju vlastoručnog potpisa. On mora osigurati autentičnost, što znači da ga može izdati samo potpisnik osobno te neporecivost, odnosno nemogućnost opovrgavanja potpisanog dokumenta.

10.3. Osnovni elementi PKI infrastrukture

Osnovne komponente PKI infrastrukture su [14]:

- Korisnici PKI infrastrukture ili krajnji entitet
- Certifikacijsko tijelo (CA – *Certificate Authority*)
- Registracijsko tijelo (RA – *Registration Authority*)
- Baza valjanih i opozvanih certifikata (CRL – *Certificate Revocation List*).
- Izdavatelj opozvanih certifikata (CRL *Issuer*)

Korisnici PKI infrastrukture mogu biti fizičke ili pravne osobe ali i hardveri (kao što su serveri i router-i) te softveri (programi i procesi), odnosno sve što može biti identificirano imenom na digitalnom certifikatu.

Certifikacijsko tijelo je ovlaštena ustanova za potpisivanje i izdavanje certifikata, obnavljanje i opoziv certifikata. CA je krovno tijelo PKI infrastrukture koje jamči ispravnost podataka u certifikatu te služi za verifikaciju identiteta krajnjih korisnika.

Registracijsko tijelo kao dio PKI infrastrukture posjeduje svoj certifikat koji ga ovlašćuje za poslove registracije korisnika ili krajnjih entiteta PKI infrastrukture.

Baza valjanih i opozvanih certifikata je sustav koji pohranjuje certifikate te listu opozvanih certifikata koji su dostupni unutarnjim ali i vanjskim korisnicima PKI infrastrukture koji koriste certifikate za identifikaciju.

Izdavač opozvanih certifikata izdaje listu opozvanih certifikata. Certifikati imaju svoj period valjanosti, pa se na toj listi nalaze certifikate čiji je rok valjanosti istekao ali i oni certifikati koji su opozvani, npr. zbog kompromitacije privatnog ključa. Lista opozvanih certifikata je javno dostupna.

Osnovni nusprodukt infrastrukture javnih ključeva je digitalni certifikat. Digitalni certifikat je digitalno potpisan dokument kojim se objavljuje javni ključ nositelja certifikata. Digitalni certifikati predstavljaju sustav razmjene javnih ključeva među korisnicima PKI infrastrukture, odnosno ovo je način da se korisnici upoznaju sa javnim ključevima i identitetom njihovih nositelja.

Digitalni certifikati minimalno sadrže slijedeće podatke:

- Serijski broj certifikata
- Verzije certifikata
- Naziv izdavatelja certifikata odnosno certifikacijskog tijela
- Valjanost certifikata
- Ime nositelja certifikata
- Javni ključ nositelja certifikata
- Digitalni potpis izdavatelja certifikata

Takav certifikat potpisan je s privatnim ključem CA-a kako bi se potvrdila vjerodostojnost certifikata te spriječilo njihovo krivotvorenje.

Tipičnu implementaciju PKI infrastrukture predstavlja hijerarhijski model povjerenja. U takvom modelu hijerarhija se sastoji od niza certifikacijskih tijela. Primjerice, u financijskom svijetu usluga, umjesto da postoji jedan CA koji potpisuje sve digitalne certifikate krajnjih korisnika, može postojati jedan CA na nacionalnoj razini koji potpisuje digitalne certifikate pojedinačnim financijskim institucijama. Tada je svaka ta institucija pojedinačni CA koji potpisuje digitalne certifikate svojih korisnika – nositelja računa. U takvoj strukturi, najviša točka povjerenja je tzv. krovni ili korijenski CA. Postoji još nekoliko različitih modela hijerarhije certifikacijskih tijela, a model kojeg propisuje ICAO za uporabu u sustavima izdavanja i provjere e-putovnica opisan je u slijedećem poglavlju.

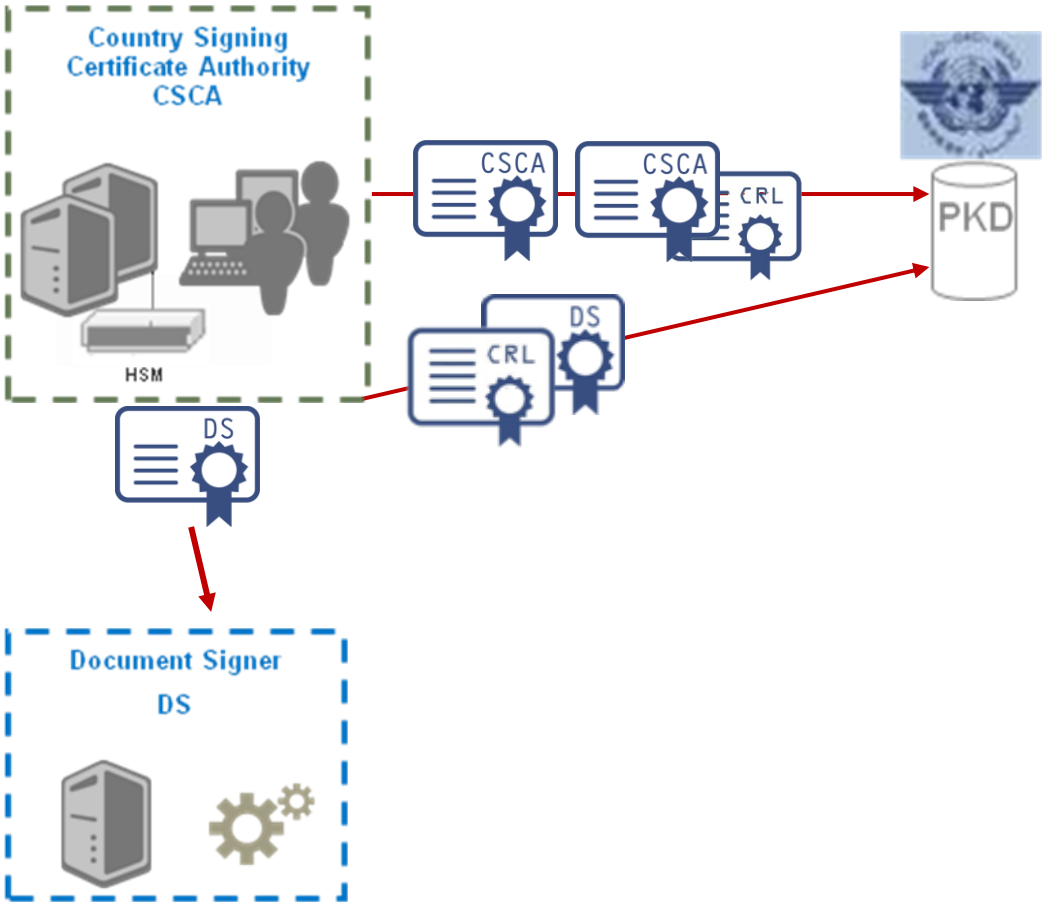
10.4. ICAO PKI model

PKI model infrastrukture za sustave e-putovnica definiran je od strane ICAO-a u svrhu internacionalne verifikacije putnih isprava te unificiranosti sustava infrastrukture javnih ključeva u raznim državama. Takav model je izrađen kako bi se osigurala što bolja i jednostavnija hijerarhija cjelokupne infrastrukture digitalnih certifikata u sustavima izdavanja, uporabe i provjere e-putovnica. Bilo je nužno osigurati da se valjanost certifikata što lakše provjeri kako bi se mogla potvrditi autentičnost te valjanost svake pojedinačne putne isprave, ali i osigurati brzu fluktuaciju putnika te nesmetano odvijanje graničnih kontrola.

10.4.1. Ovlašteno „Krovno tijelo“ države

Po ovom modelu svaka država koristi svoje vlastito samostalno okruženje koje je neovisno o drugim državama. Na najvišoj razini hijerarhije nalazi se Krovno tijelo države, nazvano **CSCA** (*Country Signing Certificate Authority*).
CSCA je ovlašteno tijelo za izdavanje certifikata za potrebe strojno čitljivih putnih dokumenata. Ono izdaje glavni certifikat za državu, $\mathbf{C_{CSCA}}$, kojeg ujedno sama ovjerava i potpisuje. Također generira par asimetričnih ključeva privatni i javni $\mathbf{KPr_{CSCA}}$ i $\mathbf{KPu_{CSCA}}$.

Certifikat krovnog tijela $\mathbf{C_{CSCA}}$ distribuira se sigurnim bilateralnim diplomatskim putem drugim državama, a također i ICAO-u jer on čini temelj provjere valjanosti certifikata potpisnika putne isprave $\mathbf{C_{DS}}$. Potpisnik putne isprave – **DS** (*Document Signer*) slijedeći je u hijerarhijskom nizu infrastrukture javnih ključeva, te se u praksi najčešće odnosi na onu instituciju koja vrši postupke personalizacije e-putovnica.
DS certifikat potpisan je privatnim ključem krovnog tijela države KPr_{CSCA} čime mu je potvrđena vjerodostojnost.
Krovno tijelo države CSCA uz certifikat potpisnika putne isprave izdaje i par ključeva potpisnika putne isprave, privatni i javni $\mathbf{KPr_{DS}}$ i $\mathbf{KPu_{DS}}$, koji se koriste za enkripciju podataka pohranjenih na čipu putne isprave.



Slika 56 – Prikaz modela PKI infrastrukture e-putovnice 1. generacije

Izradila: Željka Stražnicky, lipanj 2011.

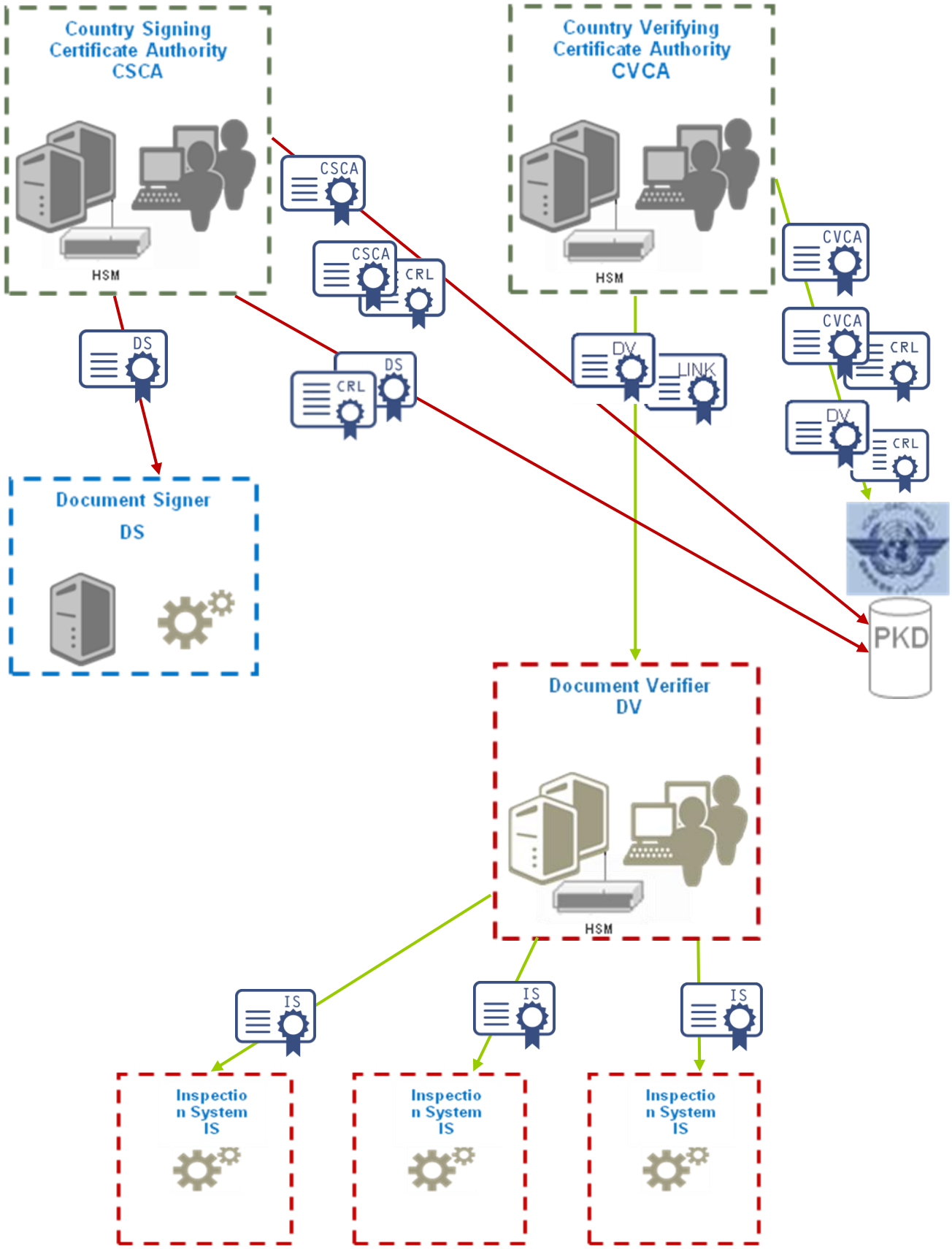
Certifikat potpisnika putne isprave **C_{DS}** mora biti pohranjen na čipu putne isprave, a svaka država ga mora proslijediti ICAO-u, te razmijeniti bilateralnim putem sa svim državama. Privatni ključ potpisnika putne isprave **KPr_{DS}** koristi se za potpisivanje sigurnosnog objekta dokumenta putne isprave koji se naziva **SO_D** (*Secure Data Object*), koji je pored DG grupa DG1 i DG2 obavezni element koji mora biti implementiran u strukturu podataka na čipu putne isprave. Element SO_D osigurava autentičnost DS certifikata, odnosno potpisnika putne isprave.

Kako bi se osigurala autentičnost pohranjenih podataka oni se pretvaraju u heksadecimalni oblik korištenjem heš funkcije te se potpisuju privatnim ključem potpisnika putne isprave KPr_{DS} i pohranjuju se u SO_D. Tako kriptirani podaci su dostupni jedino ukoliko ih se dešifrira korištenjem odgovarajućeg javnog ključa potpisnika putne isprave KPr_{DS} koji je razmijenjen bilateralnim putem s ostalim državama, a nalazi se i pohranjen u obliku certifikata u LDS aplikaciji. Nakon što su svi podaci procesom individualizacije pohranjeni na čip, on se zaključava, na način da je nemoguće naknadno upisivati dodatne podatke u njega.

Prvi korak u provjeri putne isprave na graničnom prijelazu je provjera sadržaja podataka koji se nalaze na čipu i podataka koji se nalaze na identifikacijskoj stranici.
Princip provjere bazira se na tome da se javnim ključem KPu_{DS} dekriptiraju podaci koji se nalaze u SO_D objektu. Ukoliko se odgovarajućim javnim ključem države ne može dekriptirati podatak koji se nalazi u SO_D- u, tada je za pretpostaviti da je čip putne isprave mijenjan, te da nije potpisan valjanim privatnim ključem KPr_{DS} potpisnika putne isprave. Ukoliko se podaci uspješno dekriptiraju ali njihova heš vrijednost nije identična onoj heš vrijednosti koja se dobiva iz DG1 i DG2, tada se može zaključiti da su podaci na identifikacijskoj stranici putne isprave izmijenjeni.

Kada se radi o 2. generaciji e-putovnica, koja podrazumijeva implementaciju dodatnih autentifikacijskih mehanizama, poput proširene kontrole pristupa, tada je organizacijska struktura infrastrukture javnih ključeva drugačija. U tom slučaju ona sadrži dodatni ogranak PKI infrastrukture koji se koristi za certificiranje inspekcijskih uređaja za provjeru putnih isprava na graničnim prijelazima. To znači da svaki inspekcijski uređaj sadrži svoj certifikat kojime ga se ovlašćuje za pregled putnih isprava. Ogranak PKI infrastrukture za izdavanje certifikata inspekcijskim uređajima (čitačima) nosi naziv **CVCA** (*Country Verifiing Certificate Authority*), a ispod sebe može imati jedan ili više **DV** (*Document Verifier*) podsustava.

CSCA i CVCA mogu biti integrirani u jedan entitet, no u praksi se kreira zaseban par ključeva za zasebne role.
Na slici 57 prikazana je organizacijska shema PKI infrastrukture kod sustava izdavanja i provjere e-putovnica 2. generacije.



Slika 57– Skica PKI sustava za izdavanje i provjeru putnih isprava 2. generacije

Izradila: Željka Stražnicky, lipanj 2011.

10.5. Autentifikacijski mehanizmi

Autentifikacijski ili sigurnosni mehanizmi čipa imaju ulogu zaštite podataka spremljenih na čipu te osiguranje autentičnosti, cjelovitosti i neporecivosti.

Kratki pregled vrsti autentifikacijskih mehanizama te njihovih uloga prikazan je u tablici:

MEHANIZAM	SVRHA MEHANIZMA	STATUS
PASIVNA AUTENTIFIKACIJA (PA)	Dokazuje da su certifikat izdavatelja putne isprave (DS), pa time i certifikacijskog tijela (CSCA), kao i LDS aplikacija autentični i nisu izmijenjeni.	OBAVEZNO
OSNOVNA KONTROLA PRISTUPA (BAC)	Onemogućava neovlašteno prikupljanje podataka na čipu (*skimming)*. Onemogućava presretanje podataka za vrijeme komunikacije između putovnice i čitača (*eavesdropping*).	OBAVEZNO U EU
AKTIVNA AUTENTIFIKACIJA (AA)	Dokazuje da su podaci na čipu originalni, tj. da nisu kopirani te da čip nije zamijenjen.	OPCIONALNO
PROŠIRENA KONTROLA PRISTUPA (EAC)	Onemogućava neovlašteni pristup osjetljivim biometrijskim podacima – otiscima prstiju (*skimming*). Onemogućava neovlašteno prikupljanje otisaka prstiju (*skimming*). Dokazuje da su podaci na čipu originalni, tj. da nisu kopirani te da čip nije zamijenjen.	OBAVEZNO U EU

Tablica 20 - Popis autentifikacijskih mehanizama e-putovnica

10.5.1. Pasivna autentifikacija [14]

Na čipu putovnice nalazi se LDS aplikacija koja sadrži grupe podataka (str.23). Pored LDS aplikacije čip sadrži i objekt koji se naziva **SO_D** (*Document Security Object*). SO_D objekt sadrži heš vrijednosti podataka LDS aplikacije, a također je i digitalno potpisan od strane potpisnika putne isprave (DS).

Kako bi se potvrdila autentičnost podataka LDS aplikacije, koristi se javni ključ potpisnika putnih isprava (DS) koji se nalazi pohranjen u inspekcijskom uređaju ili na čipu putovnice u jednoj od slobodnih grupa LDS aplikacije. Njime se dešifrira vrijednost SO_D objekta, a usporedbom heša SO_D i LDS-a potvrđuje se autentičnost dokumenta.

Ukoliko je sadržaj LDS-a jednak sadržaju SO_D-a tada je sigurno da su podaci na čipu autentični, tj. da nisu mijenjani. Ovom metodom nije moguće „spriječiti“ kopiranje sadržaja čipa. Za verifikaciju podataka čipa potrebna je i dodatna fizička inspekcija dokumenta od

strane osobe koja vrši provjeru na graničnim prijelazima kako bi se potvrdila autentičnost putne isprave.

Kako bi bila moguća inspekcija podataka pohranjenih na čipu putne isprave pasivnom autentifikacijom, u sustavu za inspekciju (čitačima) na graničnim prijelazima trebaju biti pohranjeni javni ključevi i certifikati države koja je izdala putnu ispravu, a čija se autentičnost provjerava. Stoga je u svakom inspekcijskom sustavu nužno dostupan certifikat krovnog tijela države $\mathbf{C_{CSCA}}$ i certifikat izdavatelja putnih isprava $\mathbf{C_{DS}}$.

Proces provjere podataka pohranjenih na čipu pasivnom autentifikacijom odvija se na slijedeći način:

- Document Security Object (SO_D) koji opcionalno sadrži Certifikat potpisnika putne isprave (C_{DS}) se čita s čipa.
- Iz SO_D-a se očitaju podaci o Izdavatelju putne isprave.
- Digitalno potpisan SO_D se verificira u inspekcijskom sustavu uz korištenje javnog ključa potpisnika putne isprave KPu_{DS}. Ovo podrazumijeva da je certifikat potpisnika putnih isprava C_{DS} koji je vezan uz dotični javni ključ pohranjen na inspekcijskom sustavu. Certifikat dodatno može biti pohranjen i na samom čipu u jednoj od slobodnih DG grupa LDS aplikacije. Kada se javnim ključem dešifrira sadržaj SO_D-a provjeravaju se podaci o tijelu koje je izdalo putovnicu te se oni uspoređuju s podacima iz certifikata koji se nalaze u inspekcijskom sustavu.
- Inspekcijski sustav očitava grupe podataka iz LDS-a.
- Djeluje se heš funkcijom na podatke iz LDS aplikacije te se dobivene vrijednosti uspoređuju s vrijednostima iz SO_D-a. Ukoliko su heš vrijednosti identične podaci koji se nalaze u LDS-u su nepromijenjeni i autentični.

Pristup otiscima prstiju na čipu je moguć jedino nakon provedene pasivne autentifikacije podataka. Iako pasivna autentifikacija može potvrditi vjerodostojnost podataka na čipu njome se ne može spriječiti njihovo kopiranje.

Kopirane podatke neke originalne putne isprave teoretski je moguće pohraniti na čip druge putne isprave. Kako bi se ovo izbjeglo potrebno je usporediti podatke nositelja putovnice koji se nalaze u grupi podataka DG1 i DG2 s podacima u strojno čitljivoj zoni te slikom na identifikacijskoj stranici putovnice. Ukoliko su podaci identični tada se može potvrditi da podaci s čipa doista odgovaraju putnoj spravi.

10.5.2. Aktivna autentifikacija - Active Authentication – AA [14]

Svaki izdavatelj putovnica može odlučiti želi li implementirati aktivnu autentifikaciju, budući da navedeni mehanizam nije obavezan element zaštite.
Upotrebom ovakvog načina autentifikacije sprječava se mogućnost zamjene čipa u putnoj ispravi. Kako bi se osiguralo da ne dođe do zamjene čipa u putnoj ispravi, između čipa putovnice i inspekcijskog uređaja pokreće se izazov-odziv protokol kojim se ostvaruje komunikacija između ta 2 entiteta, kako bi se utvrdila obostrana autentičnost i mogućnost početka međusobne sigurne komunikacije.

Za tu svrhu koriste se zasebna 2 asimetrična ključa - privatni ključ aktivne autentifikacije **KPr_{AA}** i javni ključ aktivne autentifikacije **KPu_{AA}**. Javni dio ključa aktivne autentifikacije nalazi se na poziciji DG15 LDS aplikacije, ali i u SO_D objektu, gdje se nalazi njegova heš vrijednost.
Prilikom dekriptiranja SO_D-a javnim ključem potpisnika putne isprave KPu_{DS}, potvrđuje se vjerodostojnost javnog ključa aktivne autentifikacije KPu_{AA}. Privatni ključ aktivne autentifikacije KPr_{AA} nalazi se u zaštićenoj memoriji čipa.
Provjerom autentičnosti strojno čitljive zone kroz njegovu heš vrijednost u SO_D-u, u kombinaciji sa izazov-odziv protokolom te korištenjem ključeva aktivne autentifikacije (KPu_{AA} i KPr_{AA}), inspekcijski uređaj može verificirati da su podaci iz SO_D-a očitani s originalnog čipa, odnosno originalne putne isprave. Za ovaj postupak provjere neophodna je ko-procesorska funkcionalnost čipa.

Za provođenje postupka aktivne autentifikacijske inspekcijski uređaj mora podržavati ovakvu vrstu provjere. Također, inspekcijski uređaj mora imati mogućnost optičkog čitanja strojno čitljive zone na identifikacijskoj stranici putovnice.

Postupak aktivne autentifikacije provodi se na slijedeći način:

- Inspekcijski uređaj optički čita sadržaj strojno čitljive zone (ukoliko ovo nije provedeno već kao dio mehanizma osnovne kontrole pristupa) i uspoređuje ga s informacijama pohranjenima u grupi podataka DG1.

- Postupkom pasivne autentifikacije verificirana je autentičnost i cjelovitost grupe DG15 gdje je smješten javni ključ aktivne autentifikacije. Time je osigurano da je javni ključ autentičan i nepromijenjen.

- Kako bi provjerio da SO_D objekt nije kopiran, inspekcijski sustav koristi ključeve aktivne autentifikacije u izazov-odziv protokolu. Ukoliko je protokol uspješno protekao, moguće je potvrditi da su podaci iz čipa te podaci sa identifikacijske stranice identični te da je putovnica originalna.

Inspekcijski uređaj generira nasumični izazov i šalje ga putovnici

1 ←

2 →

Putovnica potpisuje izazov sa privatnim ključem aktivne autentifikacije KPr_{AA} koji je smješten u sigurnom dijelu memorije te šalje javni dio ključa aktivne autentifikacije KPu_{AA} inspekcijskom uređaju-

3 ←

Inspekcijski uređaj verificira izazov putem dobivenog javnog ključa čime potvrđuje da se radi o autentičnom čipu.

Slika 58 – Proces aktivne autentifikacije putne isprave

10.5.3. Osnovna kontrola pristupa - Basic Access Control (BAC) [14]

Osnovni potencijalni problem kod elektroničkih putovnica je u tome što postoji mogućnost čitanja čipa s beskontaktnim čitačem bez potrebe otvaranja putovnice, ukoliko ne postoji sigurnosni mehanizam koji bi to onemogućio. Isto tako, u slučaju nekriptirane komunikacije između čipa i inspekcijskog uređaja postoji mogućnost presretanja informacija čak sa udaljenosti od nekoliko metara.

Kako bi se onemogućilo neovlašteno čitanje čipa bez pristanka nositelja putovnice ili presretanje informacija u komunikaciji s čitačem, primjenjuje se metoda pristupa podacima na putovnici pod nazivom Osnovna kontrola pristupa (Basic Access Control – BAC).

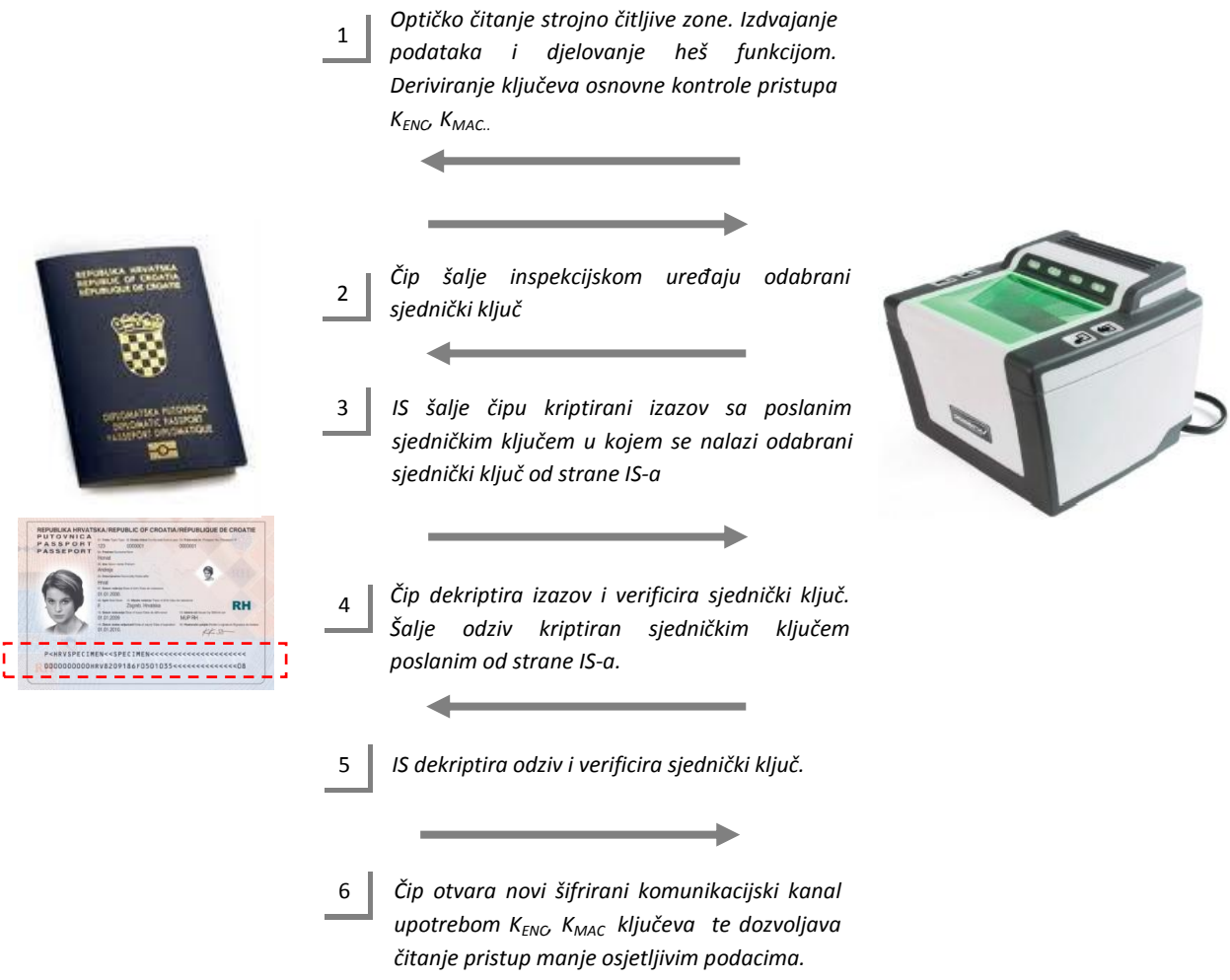
Ukoliko čip ima implementiran mehanizam osnovne kontrole pristupa on odbija pristup elektroničkim podacima, ukoliko uređaj za inspekciju ne dokaže da je autoriziran za navedeno. Autorizacija inspekcijskog uređaja izvodi se u izazov-odziv protokolu gdje čip dokazuje znanje o individualnim ključevima osnovne kontrole pristupa ($\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$) koji se izvode iz strojno čitljive zone na identifikacijskoj stranici putovnice.

Inspekcijski uređaj optički čita strojno čitljivu zonu na identifikacijskoj stranici što podrazumijeva da se putovnica otvori i položi na odgovarajući način na čitač putovnice (podrazumijeva pristanak nositelja putovnice). Ukoliko na inspekcijskom sustavu ne postoji optički čitač, tada je neophodno da se podaci iz strojno čitljive zone ručno unesu u inspekcijski uređaj. Nakon što je uspješno izvedena autorizacija inspekcijskog uređaja, čip

putne isprave pokreće kriptirani komunikacijski kanal do inspekcijskog uređaja. Zbog primijenjene kriptirane komunikacije između čipa i inspekcijskog uređaja, presretanje komunikacije je vrlo otežano. Prilikom neautoriziranih pokušaja pristupa čipu, čip odgovara „sigurnosni status nije zadovoljen“.

Postupak pristupa podacima na čipu upotrebom osnovne kontrole pristupa teče na slijedeći način:

- Inspekcijski uređaj čita podatke iz strojno čitljive zone koja sadrži broj isprave, datum i godinu rođenja, valjanost putne isprave te odgovarajuće kontrolne znamenke koristeći OCR-B čitač. Podaci strojno čitljive zone mogu se upisati i ručno, točno onako kako se pojavljuju u strojno čitljivoj zoni. Od izdvojenih podataka koji su dobiveni iz strojno čitljive zone generira se 16-bitna heš vrijednost koja čini osnovu za derivaciju ključeva osnovne kontrole pristupa (K_{ENC}, K_{MAC}).
- Inspekcijski sustav i čip prolaze kroz izazov-odziv protokol kako bi prošli uzajamnu autorizaciju nakon koje se nastavlja komunikacija šifriranim sigurnosnim kanalom.



Slika 59 – Proces osnovne kontrole pristupa (BAC)

Izradila: Željka Stražnicky, lipanj 2011.

10.5.4. Proširena kontrola pristupa – Extended Access control (EAC) [16]

Autentifikacijski mehanizam proširene kontrole pristupa ima funkcionalnost ograničenog pristupa osjetljivim podacima – otiscima prstiju. Slično kao i kod osnovne kontrole pristupa, ovim mehanizmom se uspostavlja sigurni komunikacijski kanal između čipa putovnice i inspekcijskog uređaja, ali uporabom novog para ključeva proširene kontrole pristupa.

Dok osnovna kontrola pristupa provjerava da li je inspekcijski uređaj autoriziran za pristup manje osjetljivim podacima (DG1, DG2, DG14, DG15 i SO_D), tako što zahtjeva najprije optičko čitanje strojno čitljive zone, proširena kontrola pristupa isključivo provjerava da li je inspekcijski uređaj autoriziran za pristup osjetljivim biometrijskim podacima, otiscima prstiju. Zbog navedenoga je neophodna jaka autentifikacija inspekcijskog uređaja, zbog toga se koriste jači enkripcijski ključevi nego kod osnovne kontrole pristupa.

Proširena kontrola pristupa još uvijek nije globalno zahtijevana za interoperabilne granične prijelaze (osim u EU), te stoga ovaj protokol nije specificiran od strane ICAO-a. Ovaj protokol razvila je BIG organizacija (*Brussels Interoperability Group*) te njemačko standardizacijsko tijelo – BSI (*Bundesamt fűr Sicherheit in der Informationstechnik*), a ICAO ga je prihvatio. Protokol je opisan u dokumentu *Machine Readable Travel Documents – Extended Access Control (EAC) Version 2.0 Public Beta 1 (2007-06-22)* izdanom od strane *Federal office for information security* iz Njemačke.

Proširena kontrola pristupa je kombinacija dva pod-protokola:

- **čip autentifikacije** (*chip authentication* – CA)
- **terminalske autentifikacije** ili autentifikacije inspekcijskog uređaja (*terminal authentication* – TA)

Autentifikacija čipa

Ovaj protokol je alternativa opcionalnoj aktivnoj autentifikaciji, budući da također omogućuje inspekcijskom uređaju da verificira autentičnost čipa putem verifikacije javnog dijela ključa proširene kontrole pristupa koji je spremljen u grupu DG14 te SO_D objekta u kojemu je njegova heš vrijednost.

Autentifikacija čipa ima određene prednosti u odnosu na aktivnu autentifikaciju koje proizlaze iz snažnije uspostavljenog komunikacijskog kanala zbog uporabe snažnijih enkripcijskih sjedničkih ključeva. Zbog navedenoga mnoge države koje imaju implementiranu proširenu kontrolu pristupa, ne primjenjuju mehanizam aktivne autentifikacije.

Uloga čip autentifikacije je:

- da ostvari sigurni prijenos podataka između čipa i terminala upotrebom jakih sjedničkih ključeva.
- verifikacija autentičnosti čipa, tj. dokazati da podaci nisu kopirani te da čip nije zamijenjen.

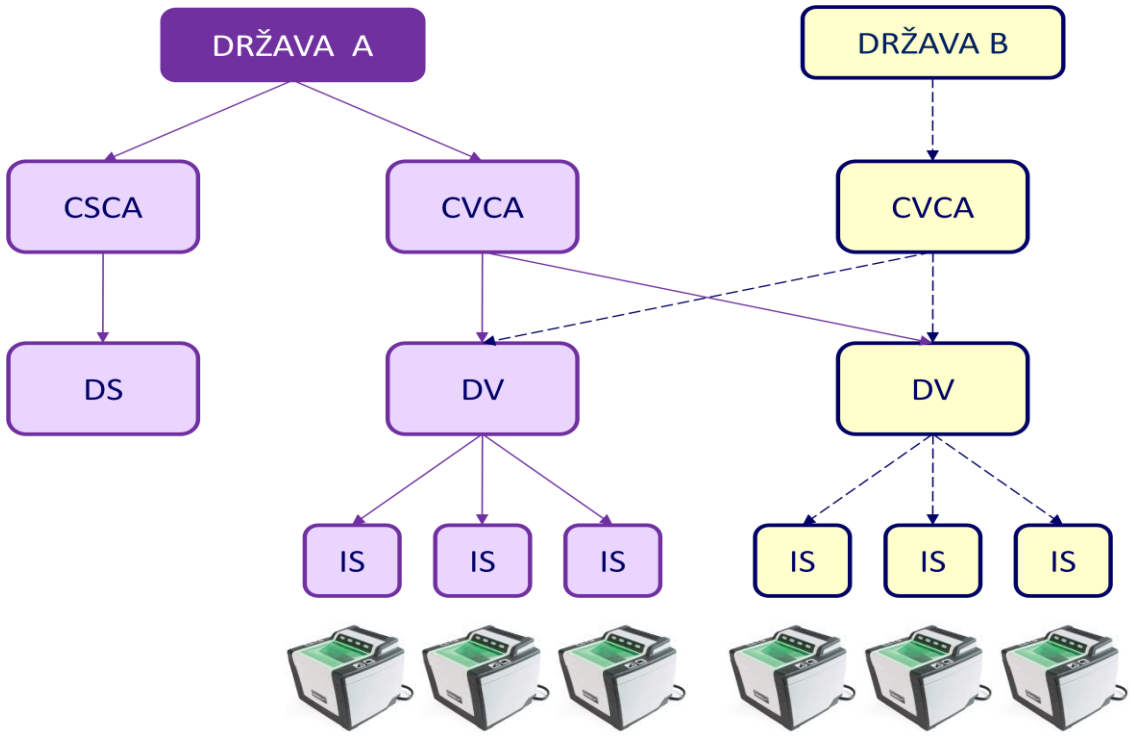
Terminalska autentifikacija

Nakon što je provedena autentifikacija čipa, slijedi autentifikacija terminala.

Terminalska autentifikacija je izazov-odziv protokol koji osigurava autentifikaciju terminala. Kako bi se terminal, odnosno inspekcijski uređaj mogao autentificirati čipu, tj. dokazati da je ovlašten za pristup osjetljivim podacima, inspekcijski uređaj mora posjedovati odgovarajući certifikat (javni ključ i korespondirajući privatni ključ) te dodijeljena prava pristupa. Certifikati se obično dodjeljuju svakom inspekcijskom uređaju u sustavu od strane PKI CVCA ogranka infrastrukture (slika 60). Nakon što je inspekcijski uređaj dokazao poznavanje privatnog ključa, čip mu dodjeljuje prava pristupa osjetljivim podacima.

PKI ogranak koji ima ulogu certificiranja i validacije inspekcijskih uređaja, te je osnova za funkcioniranje proširene kontrole pristupa, sastoji se od slijedećih entiteta:

- CVCA (*Country Verifying Certificate Authority*)
- DV (*Document Verifier*)
- IS (*Inspection System*)



Slika 60 – Razmjena certifikata inspekcijskih uređaja među državama *Izradila: Željka Stražnicky, lipanj 2011.*

CVCA je „točka povjerenja“ koja izdaje certifikate DV entitetu/ima. Ona određuje prava pristupa za sve DV-e za pristup osjetljivim podacima u svojim nacionalnim elektroničkim putovnicama. Kako bi i druge države imale pristup osjetljivim podacima putovnica matičnih država, CVCA matične države mora također ovlastiti DV entitete drugih država.

Certifikat DV-a sadrži navedene informacije o tome kojim elementima podataka ima pravo pristupa. Kako bi se umanjio rizik od krađe inspekcijskih uređaja, certifikati DV-a imaju kratak rok valjanosti.

DV je dio PKI infrastrukture koji izdaje certifikate nacionalnim inspekcijskim uređajima. Inspekcijski certifikati uglavnom imaju ista prava pristupa i rok valjanosti kao i DV certifikat, no najčešće je rok valjanosti još kraći za inspekcijske uređaje.

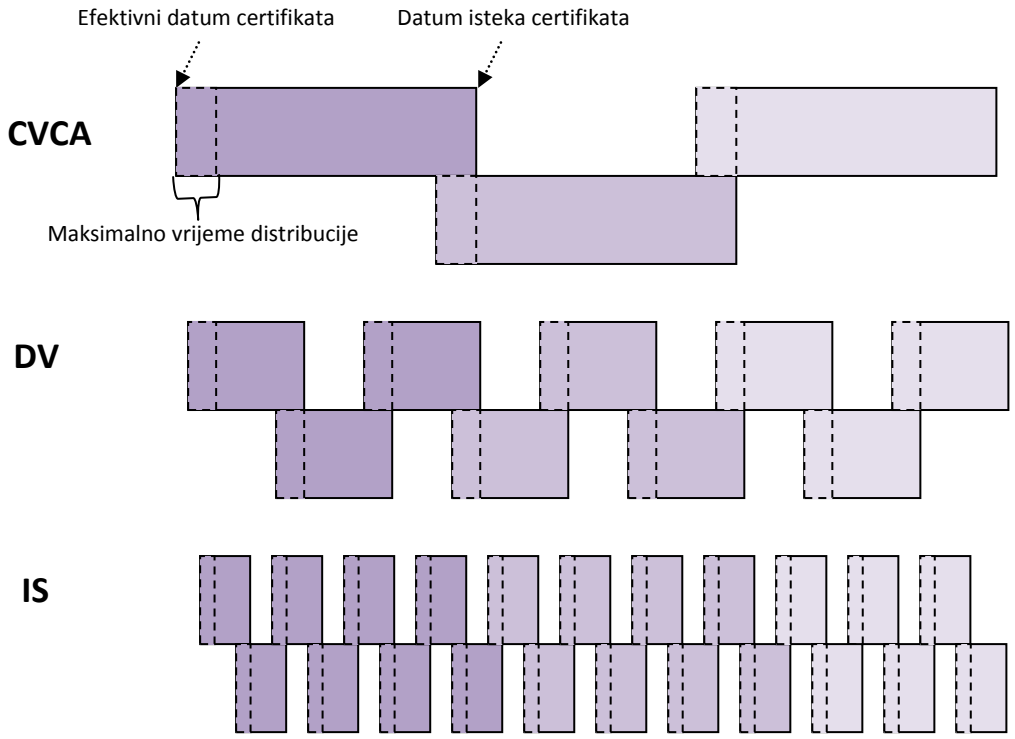
Svaki certifikat mora sadržavati period valjanosti. Period valjanosti je identificiran pomoću 2 datuma: efektivnog datuma certifikata i datuma isteka certifikata.

Efektivni datum certifikata: ovaj datum je datum generiranja certifikata.

Datum isteka certifikata: ovaj datum može biti proizvoljno odabran od strane izdavača certifikata, ali sa preporukom od najviše 30 dana za IS certifikate.

Prilikom generiranja certifikata izdavatelj mora pažljivo isplanirati obnovu certifikata, jer mora biti dovoljno vremena za prenošenje certifikata i uspostavljanje lanca certifikata. To znači da novi certifikati moraju biti generirani prije nego postojeći isteknu.

Rezultirajuće maksimalno vrijeme distribucije mora biti jednako razlici datuma isteka starog certifikata i efektivnog datuma novog certifikata (slika 61).



Slika 61 – Maksimalno vrijeme distribucije certifikata *Izradila: Željka Stražnicky, lipanj 2011.*

Politika certifikata

Svaki CVCA i DV bi trebali objaviti Politiku certifikata ili Izjavu o praksi certifikacije (*Certification practise statement*) koja definira najmanje slijedeće procedure:

- Generiranje certifikata
- Izdavanje certifikata
- Distribuciju certifikata
- Procedure oporavka (*Disaster/Recovery*)

Također se preporučuje da se definiraju ograničenja uporabe, fizička sigurnost i stupanj evaluacije uređaja koji se koriste za pohranu privatnih ključeva te za „obradu“ osjetljivih (osobnih) informacija.

Provjera valjanosti certifikata

Za provjeru valjanosti terminalskog certifikata (IS), čip mora imati dostupan lanac certifikata (*certificate chain*) koji počinje od „točke povjerenja“ odnosno krovnog certifikata. Točka povjerenja se više-manje odnosi na najnoviji javni ključ CVCA. Početni (prvi) javni ključ CVCA je pohranjen u sigurnu memoriju čipa u fazi personalizacije putovnice.

Kako se parovi ključeva CVCA mijenjaju kroz vrijeme jer imaju ograničeni rok valjanosti, tzv. CVCA link certifikati moraju biti generirani. Prilikom svake uspješne provjere elektroničke putovnice na graničnim prijelazima čip interno nadopunjuje CVCA certifikat prema primljenom valjanom linku certifikata. Link certifikat ima informacije o lancu svih izdanih certifikata.

U slučaju provjere putovnica na graničnim prijelazima drugih država, inspekcijski uređaji moraju ponuditi čipu putovnice odgovarajući link certifikata koji korespondira sa politikom certifikata njegove matične države, a u skladu sa certifikacijom DV entiteta druge države od strane CVCA entiteta njegove matične države.

Čip mora prihvatiti samo najnoviji terminalski certifikat. Budući da čip nema interni sat po kojem bi mogao procijeniti koji je certifikat najnoviji, trenutno vrijeme je procijenjeno na način da čip verificira najnoviji certifikat uzimajući u obzir trenutni datum kojeg poznaje.

Trenutni datum kojeg čip poznaje predstavlja datum personalizacije putovnice. Koristeći efektivni datum najnovijeg certifikata koji je sadržan u CVCA link certifikatu, DV certifikatu ili terminalskom certifikatu, čip procjenjuje stvarni/najnoviji datum.

Za svaki dobiveni certifikat čip izvodi slijedeće generalne radnje validacije certifikata:

- Verifikacija certifikata – digitalni potpis certifikata mora biti valjan, odnosno certifikat ne smije isteći. U tom slučaju procedura provjere se prekida.

- Usklađenje internog datuma – trenutni datum čipa mora biti nadomješten novim, najnoviji javni ključ mora biti unesen, novi CVCA mora biti aktiviran, dok CVCA koji je istekao mora biti deaktiviran.

Detaljnija procedura validacije certifikata od strane čipa je slijedeća:

- Čip verificira potpis na certifikatu. Ako je potpis netočan, verifikacija propada.
- Datum isteka certifikata se uspoređuje sa trenutnim datumom na čipu. Ako je datum isteka certifikata prije trenutnog datuma, verifikacija propada.
- Ukoliko je certifikat i javni ključ važeći, importiraju se u čip.
  Za CVCA certifikate: Novi CVCA javni ključ je dodan na listu „točke-povjerenja“ koja je spremljena u sigurnu memoriju čipa. Tada je uspostavljena nova točka-povjerenja.
  Za DV i IS certifikate: Novi DV ili IS javni ključ je privremeno importiran za slijedeću terminalsku autentifikaciju na graničnim prijelazima.
  Za CVCA, DV i nacionalne IS certifikate: Efektivni datum certifikata se uspoređuje sa trenutnim datumom čipa. Ako je trenutni datum čipa prije efektivnog datuma, trenutni datum se zamjenjuje sa efektivnim datumom.
- Istekle točke-povjerenja (CVCA certifikati) spremljene u sigurnu memoriju čipa su deaktivirane i mogu biti uklonjene iz liste točaka-povjerenja. Zbog vremenskog planiranja CVCA certifikata, najviše dva CVCA certifikata trebaju biti spremljena na čip.

Procedure provjere e-putovnica na graničnim prijelazima [16]

Inspekcijski sustav može koristiti standardnu inspekcijsku proceduru za pristup manje osjetljivim podacima e-putovnice ili naprednu inspekcijsku proceduru za pristup manje osjetljivim i osjetljivim podacima e-putovnice.

Kod standardne provjere putovnice, strojno čitljiva zona bi trebala biti poznata inspekcijskom uređaju (budući da je osnovna kontrola pristupa (BAC) preporučena, a obavezna je samo u EU).

Kod napredne provjere putovnice, strojno čitljiva zona mora biti poznata inspekcijskom uređaju (strojno čitljiva zona se mora optički očitati na inspekcijskom uređaju prilikom provjere putovnice).

Standardna procedura provjere e-putovnica sastoji se od slijedećih koraka:

1. e-putovnica je smještena na inspekcijski uređaj. Odabire se aplikacija e-putovnice (OBAVEZNO) – Čip ne smije dozvoliti pristup podacima e-putovnice (osim generalnim sistemskim podacima).

2. Osnovna kontrola pristupa (OPCIONALNO) – ovaj se postupak zahtjeva ukoliko ga čip omogućava. Ukoliko je omogućeno čip radi slijedeće:
    - Započet će proces komuniciranja putem šifriranog kanala.
    - Biti će omogućen pristup manje osjetljivim podacima u čipu (DG1, DG2, DG14, DG15, SO_D)

3. Pasivna autentifikacija (OBAVEZNO) – inspekcijski uređaj mora pročitati i verificirati $SO_{D.}$

4. Aktivna autentifikacija (OPCIONALNO) – ukoliko je omogućena, inspekcijski uređaj mora pročitati i verificirati DG15 i izvesti postupak aktivne autentifikacije.

5. Pristup i autentifikacija podataka – inspekcijski uređaj može pročitati i verificirati grupe podataka koje sadrže manje osjetljive podatke (svi dostupni podaci osim podataka u grupama DG3 i DG4).

<u>Napredna procedura provjere e-putovnica sastoji se od slijedećih koraka:</u>

Napredna procedura provjere može biti korištena samo za e-putovnice 2. generacije.

1. e-putovnica je smještena na inspekcijski uređaj. Odabire se aplikacija e-putovnice (OBAVEZNO) – Čip ne smije dozvoliti pristup podacima e-putovnice (osim generalnim sistemskim podacima).

2. Osnovna kontrola pristupa (OPCIONALNO) – ovaj se postupak zahtjeva ukoliko ga čip omogućava. Ukoliko je omogućeno čip radi slijedeće:
    - Započet će proces komuniciranja putem šifriranog kanala.
    - Biti će omogućen pristup DG14 koji sadrži javni ključ čip autentifikacije.
    - Biti će omogućen pristup drugim manje osjetljivim podacima (npr. DG1, DG2, DG15, SO_D).

3. Čip autentifikacija (OBAVEZNO) – inspekcijski uređaj treba pročitati DG14 i započeti čip autentifikaciju. Čip obavlja slijedeće:
    - Započet će proces komuniciranja putem šifriranog kanala upotrebom jačih enkripcijskih ključeva.

    Nakon uspješne čip autentifikacije jaka sjednička enkripcija čini nemogućim dekripciju prisluškivane komunikacije. Ipak, samo nakon provođenja i uspješne pasivne autentifikacije čip se može smatrati originalnim.

4. Pasivna autentifikacija (OBAVEZNO) – terminal će pročitati i verificirati SO_D i verificirati DG14.

5. Aktivna autentifikacija (OPCIONALNO) – ukoliko je omogućena, terminal mora pročitati i verificirati DG15 i izvesti postupak aktivne autentifikacije.

6. Terminalska autentifikacija (UVJETNO) – ovaj korak je zahtjevan za pristup osjetljivim podacima (otiscima prstiju).

    - U prvom koraku inspekcijski uređaj mora prezentirati čipu odgovarajući lanac certifikata (CVCA-DV-IS).
    - Lanac certifikata je verificiran od strane čipa korištenjem CVCA javnog ključa koji je spremljen u sigurnu memoriju čipa. Ukoliko je verifikacija uspješna predstavljenom lancu certifikata se može „vjerovati“.
    - Privatnim ključem inspekcijskog uređaja koji je pohranjen u sigurni dio inspekcijskog sustava (HSM uređaj – *Hardware security module*) inspekcijski uređaj potpisuje izazov te ga šalje čipu putovnice. Čip verificira izazov koristeći javni dio ključa kojeg je importirao putem IS certifikata.
    - čip dozvoljava pristup grupama podataka prema definiranim terminalskim pravima navedenima u certifikatu.

7. Čitanje i autentifikacija podataka – terminal može pročitati i verificirati grupe podataka prema terminalskim pravima pristupa.

8. Otisci prstiju su poslani u inspekcijski uređaj.

9. Nositelj putovnice za to vrijeme skenira otiske svojih prstiju na čitaču otisaka prstiju kojeg mu službenik predoči. Otisci prstiju se konvertiraju u odgovarajuće biometrijske predloške koristeći određeni algoritam kako bi bili isti predlošcima pohranjenima na čipu.

10. Biometrijski softver uspoređuje sve predloške i obzirom na pred-definirani prag tolerancije određuje da li su uzeti otisci prstiju kompatibilni.

ICAO PKD - direktorij javnih ključeva

Kako bi se efikasno razmijenili certifikati potpisnika putnih isprava (C_{DS}) između svih država članica, ICAO je razvio zajednički centralni direktorij pod nazivom ICAO PKD (*Public Key Directory*).

ICAO PKD ima ulogu pohranjivanja javnih ključeva potpisnika putnih isprava na jednom centralnom mjestu kako bi svim državama članicama bili pravovremeno dostupni. Javni ključevi potpisnika putnih isprava koriste se za verifikaciju i autentifikaciju putnih isprava na graničnim prijelazima te iz istog razloga moraju biti dostupni svim državama.

ICAO PKD također pohranjuje link certifikate krovnog tijela države (CSCA), ali ih koristi i za provjeru autentičnosti i cjelovitosti certifikata potpisnika putne isprave (DS) prije nego li ih pohrani u direktorij. ICAO PKD se smatra primarnim mehanizmom distribucije certifikata

potpisnika putnih isprava, no to države članice ne sprječava da navedene certifikate razmijene sa ostalim državama i bilateralnim putem.

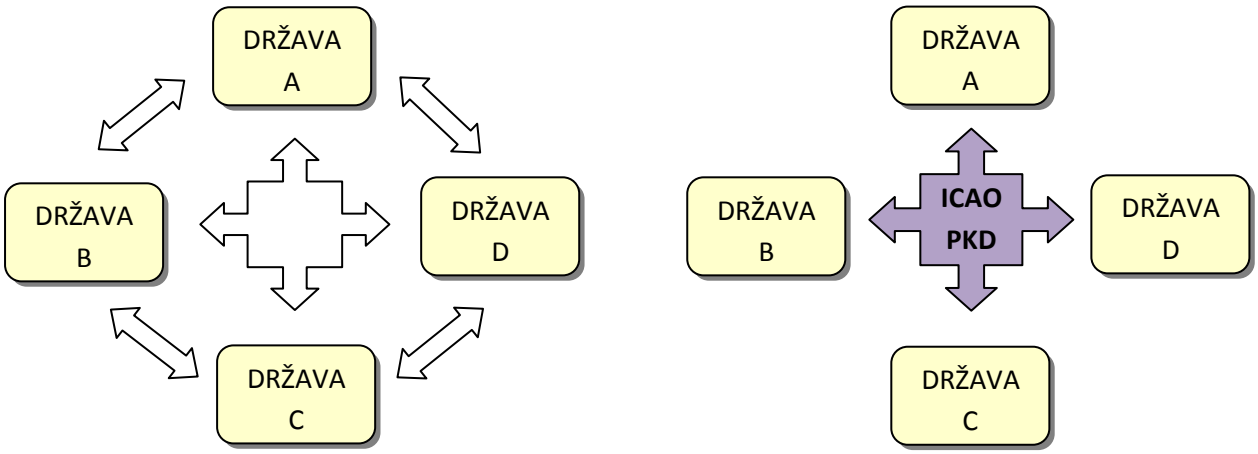
ICAO PKD je također i repozitorij lista povučenih certifikata – CRL lista svih država članica. U ovom slučaju se ICAO PKD smatra sekundarnim mehanizmom distribucije CRL lista, dok je primarni mehanizam distribucije bilateralni put.

Kod mehanizma bilaterne razmjene certifikata i CRL lista svaka država bi sa svakom državom trebala učestalo izmjenjivati podatke o korištenim javnim ključevima potpisnika putne isprave $KPr_{DS,}$ što bi zahtijevalo konstanto održavanje komunikacije u oba smjera.

Dodatan problem javio bi se na mjestima provjere putnih isprava, kao što su državne ustanove ili zrakoplovne luke, ukoliko im važeći javni ključevi ne bi bili dostavljani pravovremeno i redovito.

Jedan od načina dostupnosti javnog ključa potpisnika putne isprave KPr_{DS} može se osigurati na način da je on pohranjen u LDS aplikaciju putne isprave, što nije obavezno ali neke države primjenjuju. Ukoliko bi samo čip imao informaciju o javnom ključu potpisnika putne isprave tada postoji opasnost od nemogućnosti otkrivanja krivotvorene putne isprave. U tom slučaju bi krivotvoritelj mogao izraditi putovnicu s čipom na koju bi stavio svoje podatke te bi ju potpisao privatnim ključem kojeg je sam generirao. Prilikom provjere putne isprave s javnim ključem pohranjenim samo na čip moglo bi se zaključiti da je ona autentična.

Iz navedenih razloga odlučeno je da se uspostavi centralni direktorij javnih ključeva PKD koji će nuditi sigurnosnu infrastrukturu za pohranu i distribuciju ključeva. No, odgovornost svake države je u tome da očuva integritet privatnih ključeva koji korespondiraju javnom ključu potpisnika putne isprave te da osiguraju da su samo zadnji važeći ključevi u pravo vrijeme dostupni u direktoriju. Također, odgovornost država je i da alarmiraju onda kada ključevi budu kompromitirani.

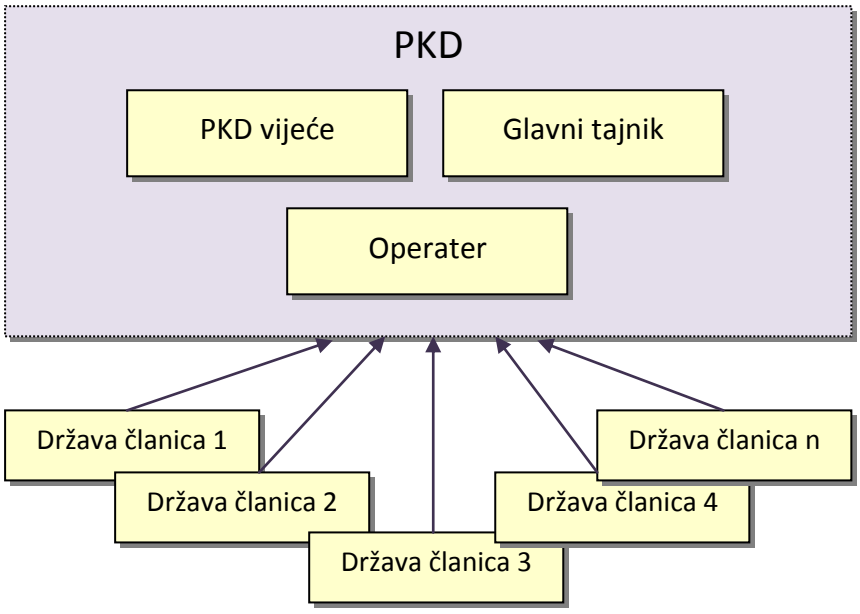


Slika 62 – Razmjena javnih ključeva između država bilateralnim putem i pomoću PKD direktorija javnih ključeva. *Izradila: Željka Stražnicky, lipanj 2011.*

10.5.5. Odgovornosti ICAO PKD-a

Odgovornosti ICAO-a vezane uz PKD su slijedeće:

- uspostavlja PKD te održava njegovu funkcionalnost i dostupnost
- redovito objavljuje i propagira PKD regulativu, procedure te specifikacije za pristup PKD-u
- pod vodstvom glavnog tajnika, te u konzultacijama sa operaterom (entitetom koji operativno održava PKD direktorij) i vijećem PKD-a, objavljuje naknade za korištenje PKD direktorija
- objavljuje nove verzije memoranduma o razumijevanju kojeg potpisuju članice PKD-a
- administrativna i operativna podrška PKD vijeću
- provodi verifikaciju i provjeru autentičnosti certifikata potpisnika putne isprave, link certifikata krovnog tijela države (izdavatelja), master CSCA liste i CRL liste te ih pohranjuje u PKD
- provodi provjeru tehničke usklađenosti certifikata sa specifikacijama objavljenima u ICAO 9303 dokumentu
- djeluje kao posrednik između članica i operatera u zaprimanju naknada



Slika 63 - Organizacijska struktura PKD-a

PKD vijeće

PKD vijeće je počelo sa svojim radom 2007 god. I tada je izabrano prvo vijeće od 15 članova na period od 3 godine. PKD vijeće između sebe bira predsjednika vijeća. Uloga vijeća je

upravljati i nadgledati aktivnosti PKD-a, povezati se sa ostalim interesnim skupinama, uključujući operativni dio graničnih prijelaza kako bi dobili dobre povratne informacije vezane uz uporabu PKD-a u praksi, praćenje statističkih podataka povezanih s brojem izdanih putovnica pojedine države, te brojem putnika koji putuju preko graničnih prijelaza i sl.

Vijeće PKD-a sastaje se 3 puta godišnje i to u Berlinu (ožujak), Pragu (lipanj) i Tokiu (listopad).

Operater

Glavni i pričuvni PKD direktorij operativno održava tvrtka NETrust Pte. Ltd iz Singapura do 2012.god. kada će se ponovno auditirati tvrtka te eventualno revidirati odluka.

Države članice

Trenutno je 25 članica PKD-a i to: AUS, AUT, CAN, CHN, CZE, FRA, D, HGK, IND, JPN, KAZ, LVA, MAC, MAR, MLD, NZL, NGA, KOR, SGP, SVK, CHE, UKR, ARE, GBR, USA.

PKD nakade

Naknade za pristup i korištenje PKD-a ovise o broju država članica, ukupni troškovi PKD-a raspoređuju se prema broju članova pa što je taj broj veći to jedinični trošak po državi članici manji. U slučaju pristupa novih članica, naknade se revidiraju.

PKD članica plaća jednokratnu registracijsku naknadu u iznosu od 56.000 $.

Godišnja naknada se sastoji iz 2 dijela: ICAO dio i PKD operaterski dio. Prema obračunu troškova za ICAO dio svaka država članica plaća godišnje 14.032 $, dok za tehnički dio (operaterski dio) plaća 43.000 $ godišnje.

Za nove izdavatelje koji žele uspostaviti testni link sa PKD direktorijem radi odgovarajuće integracije te podrške od strane operatera postoji naknada u iznosu od 9.600 $ jednokratno, a vrijedi 6 mjeseci.

Odgovornosti Izdavatelja putnih isprava (CSCA)

Odgovornosti izdavatelja putnih isprava koji su članice PKD-a su slijedeće:

- pravovremeno dostavljanje certifikata i CRL liste
- odgovornost za slanje odgovarajućih certifikata i CRL liste
- obavještavanje o kompromitaciji relevantnih privatnih ključeva
- plaćanje definiranih naknada PKD-a

Za potpisivanje i šifriranje podataka u putnim ispravama potrebno je koristiti privatne ključeve za one putne isprave koje će biti izrađene u vrijeme važenja ključeva (valjanost ključeva je vremenski limitirano).

Kako bi se odredila valjanost ključeva prijedlog ICAO-a je da svaka država odredi trajanje svojih certifikata i ključeva prema valjanosti putne isprave, te su prema tome ponuđene tri opcije na izbor izdavateljima.

Primjer 1

RAZDOBLJE	VRIJEME TRAJANJA CERTIFIKATA
Izdavanje s Privatnim ključem Potpisnika putne isprave (KPr_{DS})	1 mjesec
Valjanost putne isprave	5 godina
Valjanost certifikata Potpisnika putne isprave (C_{DS})	5 godina
Izdavanje s Privatnim ključem od CSCA (KPr_{CSCA})	3 godine
Valjanost certifikata ovlaštenog krovnog tijela (C_{CSCA})	8 godina

Tablica 21 – Mogućnosti definiranja vremena trajanja certifikata prema ICAO standardu

Primjer 2

RAZDOBLJE	VRIJEME TRAJANJA CERTIFIKATA
Izdavanje s Privatnim ključem Potpisnika putne isprave (KPr_{DS})	2 mjeseca
Valjanost putne isprave	10 godina
Valjanost certifikata Potpisnika putne isprave (C_{DS})	10 godina
Izdavanje s Privatnim ključem od CSCA (KPr_{CSCA})	4 godine
Valjanost certifikata ovlaštenog krovnog tijela (C_{CSCA})	14 godina

Tablica 22 - Tablica 21 – Mogućnosti definiranja vremena trajanja certifikata prema ICAO standardu

Primjer 3

RAZDOBLJE	VRIJEME TRAJANJA CERTIFIKATA
Izdavanje s Privatnim ključem Potpisnika putne isprave (KPr_{DS})	3 mjeseca
Valjanost putne isprave	10 godina
Valjanost certifikata Potpisnika putne isprave (C_{DS})	10 godina
Izdavanje s Privatnim ključem od CSCA (KPr_{CSCA})	5 godine
Valjanost certifikata ovlaštenog krovnog tijela (C_{CSCA})	15 godina

Tablica 23 - Tablica 21 – Mogućnosti definiranja vremena trajanja certifikata prema ICAO standardu

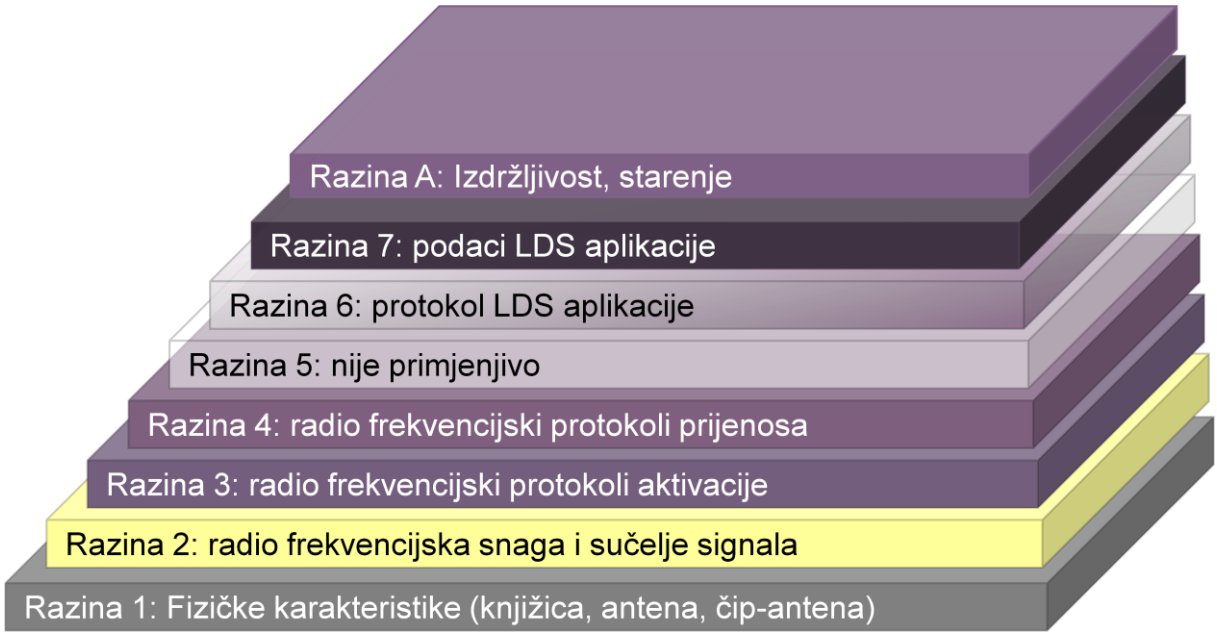
U primjerima su navedene valjanosti DS certifikata od 1, 2 ili 3 mjeseca što znači da će sve putovnice proizvedene u tom periodu biti digitalno potpisane sa istim privatnim ključem. U slučaju kompromitacije privatnog ključa, izdavatelj mora upozoriti države na pojačanu i dodatnu kontrolu putovnica potpisanih sa navedenim ključem (definirani serijski brojevi putovnica) ili će povući svu količinu putovnica i izraditi nove.

Valjanost CVCA, DV i IS certifikata svaka država ima pravo definirati za samostalno uz preporuku ICAO-a da valjanost DV i IS certifikata bude znatno kraća od valjanosti CVCA certifikata. Valjanost DV i IS certifikata može biti jednaka, no najčešće IS certifikati imaju kraću valjanost i do 30 dana.

11. EKSPERIMENTALNI DIO MAGISTARSKOG RADA

11.1. Uvod

Ispitivanja e-putovnica definirana ICAO standardom dijele se na nekoliko razina:



Slika 64 - Razine testiranja e-putovnice definirane od strane ICAO-a

Prvu grupu testiranja čine razine od 1-4, a sve su vezane uz ispitivanje radio frekvencijskog sučelja putovnice kao i protokola aktivacije u komunikaciji između čitača i čipa.

Drugu grupu testiranja čine razina 6 i 7 koje se odnose na LDS aplikaciju pohranjenu u čip putovnice.

Zadnju grupu testiranja putovnica čine testiranja razine A koja se odnose na provjeru funkcionalne sukladnosti putovnice sa ICAO standardom *„Durability of Machine Readable Passports“*, Machine Readable Travel Documents, Technical Report version: 3.2, date: 2006-08-30.

Unutar razine A, ICAO standard definira slijedeće testne metode:

- **Termalna ciklička metoda** (*Thermal cycling method*)– ovom metodom putovnice su izložene dvama temperaturnim ekstremima kroz kratak period. Ova metoda simulira termalni šok kojeg putovnica može doživjeti očitovanu kroz ekspanziju ili kontrakciju pojedinih komponenata putovnice.

- **Metoda utjecaja temperature skladištenja** (*Storage temperature stress method*) – ovom metodom se aplicira visoka ili niska temperatura i vlažnost kroz duži period. Ovom metodom simulira se izlaganje dokumenta rzanim uvjetima skladištenja.
- **Metoda utjecaja operativne temperature** (*Operational temperature stress method*) – ovom metodom se aplicira visoka ili niska temperatura i vlažnost kroz duži period. Ovom metodom simulira se izlaganje dokumenta rzanim uvjetima skladištenja.
- **Metoda djelovanja definiranom silom** (*Impact stress method*) – ovom metodom aplicirana je definirana sila kako bi se simuliralo pečatiranje na graničnim prijelazima.
- **Metoda stražnjeg džepa** (*Back pocket stress method*) – ovom metodom aplicira se definirana sila na putovnica koja simulira silu prilikom sjedanja na putovnicu kada se ona nalazi u stražnjem džepu hlača.
- **Metoda dinamičkog savijanja putovnice** (*Dynamic bend stress method*) – svrha ove metode testiranja je utvrditi izmjeničnu dinamičnu izdržljivost putovnice.
- **Metoda torzijskog zamora** (*Torsion stress method*) - svrha metode testiranja je odrediti nepovoljan mehanički ili funkcionalni efekt kod e-putovnica koji proizlazi iz torzijskog zamora.
- **Metoda okretanja stranice knjižnog bloka** (*Sheet turning stress method*) – svrha metode testiranja je utvrditi otpor papirnate stranice knjižnog bloka na savijanje u hrptu putovnice.
- **Metoda povlačenja stranice knjižnog bloka** (*Sheet pull stress method*) – svrha metode testiranja je utvrditi otpor na kidanje stranica knjižnog bloka.
- **Metoda abrazije** (*Abrasion stress method*) – svrha metode testiranja je utvriti efekt djelovanja mehaničke abrazije na identifikacijsku stranicu putovnice.
- **Metoda djelovanja olovkom** (*Pen stress method*) – svrha metode testiranja je simulirati pisanje na stranicama knjižnog bloka te utjecaj na identifikacijsku stranicu (čip, antenu).
- **Metoda evaluacije otpornosti na kemikalije** (*Resistance to chemicals evaluation method*) – svrha metode testiranja je utvrditi utjecaj kemikalija na komponente putovnice.
- **Metoda djelovanja dnevnog svjetla** (*Artificial daylight exposure stress method*) – svrha metode testiranja je utvrditi otpor na blijeđenje otiska.
- **Metoda djelovanja x-zraka** (*X-ray stress method*) – svrha metode testiranja je utvrditi utjecaj x-zraka na segmente putovnice kojima putovnica može biti izložena tijekom čitanja na optičkim čitačima.

11.2. Svrha testiranja

Svrha testiranja je utvrditi eventualnu razliku u kvaliteti i funkcionalnost e-putovnica očitovanu kroz ispravnost/ne-ispravnost rada čipa s obzirom na medij za smještaj beskontaktnog čipa, primjenom odabranih mehaničkih testova definiranih referentnim ICAO standardom [31].

Ovaj standard osigurava set instrukcija za evaluaciju prototipa putovnice koja sadržava beskontaktni čip. Evaluacija prototipa predstavlja instrument kojim se prikazuje sposobnost specifičnog tipa dokumenta da ispuni zahtjeve svakodnevne uporabe kroz njegov životni vijek. Ona prikazuje minimalni kriterij koji treba biti ispunjen kako bi se ispunilo zahtjeve ICAO-a za očekivanom izdržljivošću dokumenta.
Set testova definiranih standardom može se koristiti za evaluaciju karakteristika ne-personaliziranih e-putovnica, personaliziranih e-putovnica ili nekih materijala koji se koriste za izradu putovnica u svrhu evaluacije prototipa putovnica, evaluacije prihvatljivosti isporuke (između onog proizvođača koji proizvodi knjižicu putovnice i onoga koji vrši personalizaciju putovnice) ili za neku drugu svrhu.

11.3. Primijenjene metode testiranja

U procesu testiranja primijenjene su metode:

- testiranja torzijskim zamorom putovnica - *Torsion stress testing (T)*
- testiranje dinamičkim savijanjem putovnica - *Dinamic bending testing (DB)*
- testiranje djelovanjem direktne sile na putovnicu - *Impact stress testing (I)*

Mogućnost broja primijene metoda određena je brojem prikupljenih uzoraka za testiranje.

11.4. Mjesto testiranja te oprema

Testiranje je obavljeno u tvrtki AKD d.o.o te na opremi u njezinom vlasništvu.

Korištena hardverska testna oprema je slijedeća:

- **PPT 2007/T** proizvođača Muehlbauer AG (Njemačka) - *Torsion stress testing* - testiranje torzijskim zamorom putovnica.
- **PPT 2007/DB** proizvođača Muehlbauer AG (Njemačka) – *Dinamic bending testing* - testiranje dinamičkim savijanjem putovnica.
- **PPT 2007/I** proizvođača Muehlbauer AG (Njemačka) – *Impact stress testing* – testiranje djelovanjem definirane sile na putovnicu kako bi se simuliralo pečatiranje na graničnim prijelazima.
- **Beskontaktni čitač – OMNIKEY CARDMAN 5321**

Korištena softverska testna oprema je slijedeća:

- **Eclipse**

11.5. Testni materijal

Korišteni testni materijal su knjižice e-putovnica 2 osnovna tipa:

- e-putovnica s PC stranicom sa čipom – ukupno 2 različita proizvođača PC stranica
- e-putovnice s čipom u koricama – ukupno 2 različita proizvođača e-korica

OZNAKA GRUPE TESTIRANIH PUTOVNICA	MEDIJ U KOJEM JE POHRANJEN ČIP	OPIS MEDIJA	UVEZ
PUTOVNICA A	PC STRANICA	Višeslojna PC stranica, debljine cca. 1mm, sa polipropilenskom (PP), ultrasonično varenom hrptenom trakom.	PC stranice inozemnog dobavljača A, uvezane u knjižicu putovnice u AKD-u na liniji za uvez putovnica - Kugler.
PUTOVNICA B	PC STRANICA	Višeslojna PC stranica, debljine cca. 1 mm, sa hrptenim materijalom (slično materijalu za brodsko jedro) spojenim kemijskim i mehaničkim putem sa PC materijalom.	PC stranice inozemnog dobavljača B, uvezane u knjižicu putovnice u AKD-u na liniji za uvez putovnica - Kugler.
PUTOVNICA C	E-KORICE	Višeslojne korice bazirane na papirnatom materijalu i čipu s bakrenom antenom.	E-korice inozemnog dobavljača C, uvezane u knjižicu putovnice u AKD-u na liniji za uvez putovnica - Kugler.
PUTOVNICA D	E-KORICE	Višeslojne korice bazirane na papirnatom materijalu i čipu s bakrenom antenom.	E-korice inozemnog dobavljača D, uvezane u knjižicu putovnice u AKD-u na liniji za uvez putovnica - Kugler.

Tablica 24 – Opis osnovnih karakteristika medija za pohranu čipa testiranih proizvođača

11.6. Testna količina putovnica

U tablici je prikazan pregled količina korištenih putovnica za testiranje prema tipu testiranja i prema grupi u koju spadaju putovnice s obzirom na medij za smještaj čipa te proizvođača tog medija. Za svaki pojedini test korištene su zasebne putovnice, namijenjene samo za tu vrstu testa, što znači da su 4 putovnice bile izložene samo jednoj vrsti mehaničkog djelovanja.

	BROJ PUTOVNICA PO TESTU			
	DINAMIC BENDING (DB)	**TORSION STRESS (T)**	**IMPACT STRESS (I)**	UKUPNO
PUTOVNICA A	4	4	4	**12**
PUTOVNICA B	4	4	4	**12**
PUTOVNICA C	4	4	4	**12**
PUTOVNICA D	4	4	4	**12**
UKUPNO	**16**	**16**	**16**	**48**

Tablica 25 – Popis broja putovnica po testu te proizvođačima

11.7. Plan testiranja

U tablici je prikazan plan testiranja s obzirom na broj ponavljanja mehaničkog utjecaja na putovnice po pojedinom testu. U tablici je naznačen i minimalni broj ponavljanja mehaničkog utjecaja pojedinog testa kojeg e-putovnica mora „izdržati“ kako bi se smatrala funkcionalnom i izdržljivom prema ICAO standardu.

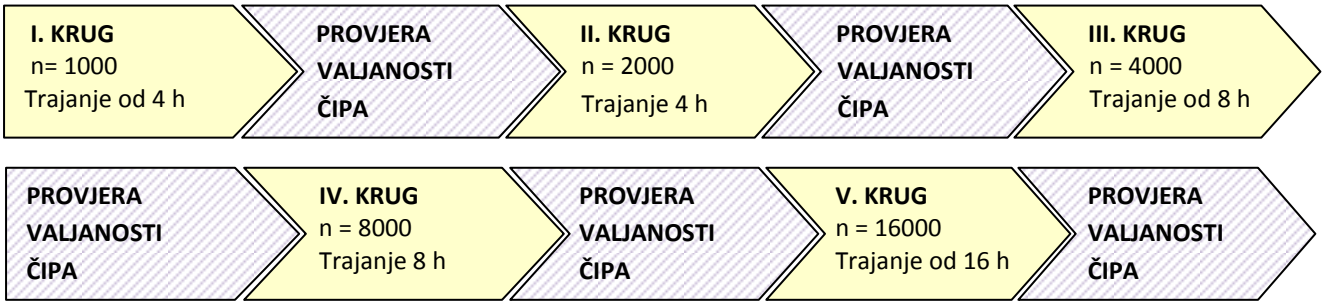
BROJ PONAVLJANJA PO TESTU					
	DB	**T**	**I**		PROVJERA FUNKCIONALNOSTI ČIPA
I. KRUG	1000	500	4	Minimum / Standard	DA
II. KRUG	2000	1000	8	povećanje za 100 %	DA
III. KRUG	4000	2000	16	povećanje za 400 %	DA
IV. KRUG	8000	4000	32	povećanje za 800 %	DA
V. KRUG	16000	8000	64	povećanje za 1600 %	DA

Tablica 26 – Popis broja ponavljanja po testu

11.8. Tijek testiranja

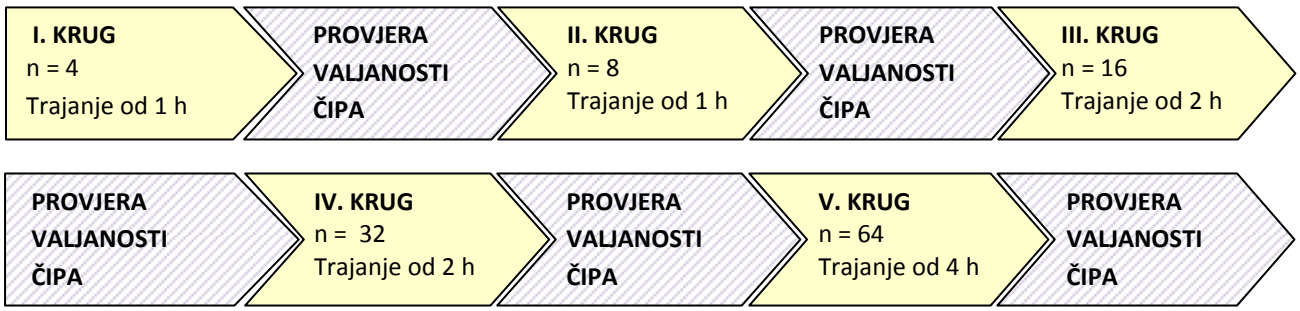
11.8.1. Test dinamičnog savijanja - Dinamic bending

Vremensko trajanje testa po grupi putovnica = 40 h
Ukupno vremensko trajanje testa za sve 4 grupe putovnica = 40 * 4 = **160 h**



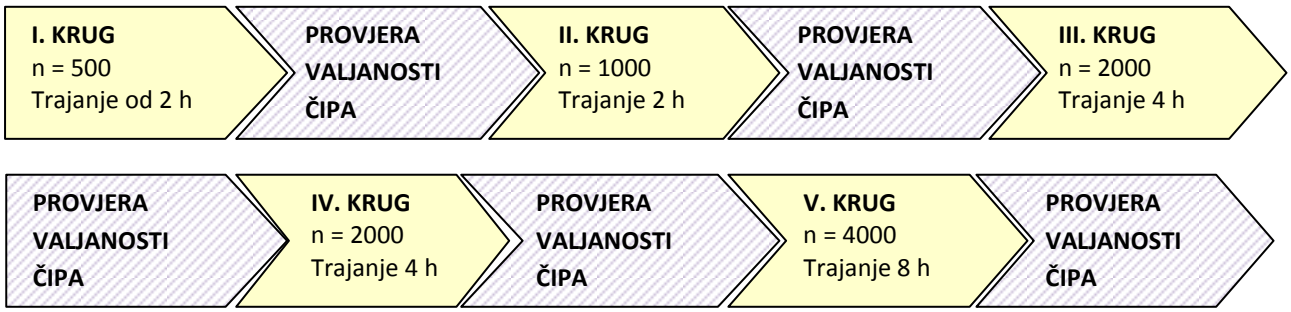
11.8.2. Test utjecaja sile - Impact stress

Vremensko trajanje testa po grupi putovnica – 10 h
Vremensko trajanje testa za sve 4 grupe putovnica = 10 * 4 = **40 h**



11.8.3. Test torzijskog zamora - Torsion stress

Vremensko trajanje testa po grupi putovnica = 20 h
Vremensko trajanje testa za sve 4 grupe putovnica = 20 * 4 = **80 h**



11.9. Opis metoda testiranja

11.9.1. Test dinamičnog savijanja putovnica - Dinamic bending

Svrha testa

Svrha testa je utvrditi izdržljivost knjižice e-putovnice na izmjenično dinamično savijanje.

Uređaj za testiranje

Korišteni uređaj za testiranje dinamičkog savijanja putovnica je **PPT 2007/DB** proizvođača Muehlbauer AG (Njemačka). U uređaj se istovremeno mogu smjestiti maksimalno 4 putovnice.

Karakteristike uređaja

Visina:	280 mm
Širina:	552 mm
Dubina:	593 mm
Težina:	cca. 37,4 kg
Napon:	230 V
Snaga:	250 W
Jačina struje:	6 A
Jačina zvuka:	max. 55,7 dB (A)

Tablica 27 – Karakteristike uređaja PPT 2007/DB

Testni preduvjeti

Temperatura okoline:	23˚C ± 5˚ C
Relativna vlažnost:	40 % - 60 %

Tablica 28 – Zahtijevani testni preduvjeti

Ulazni parametri

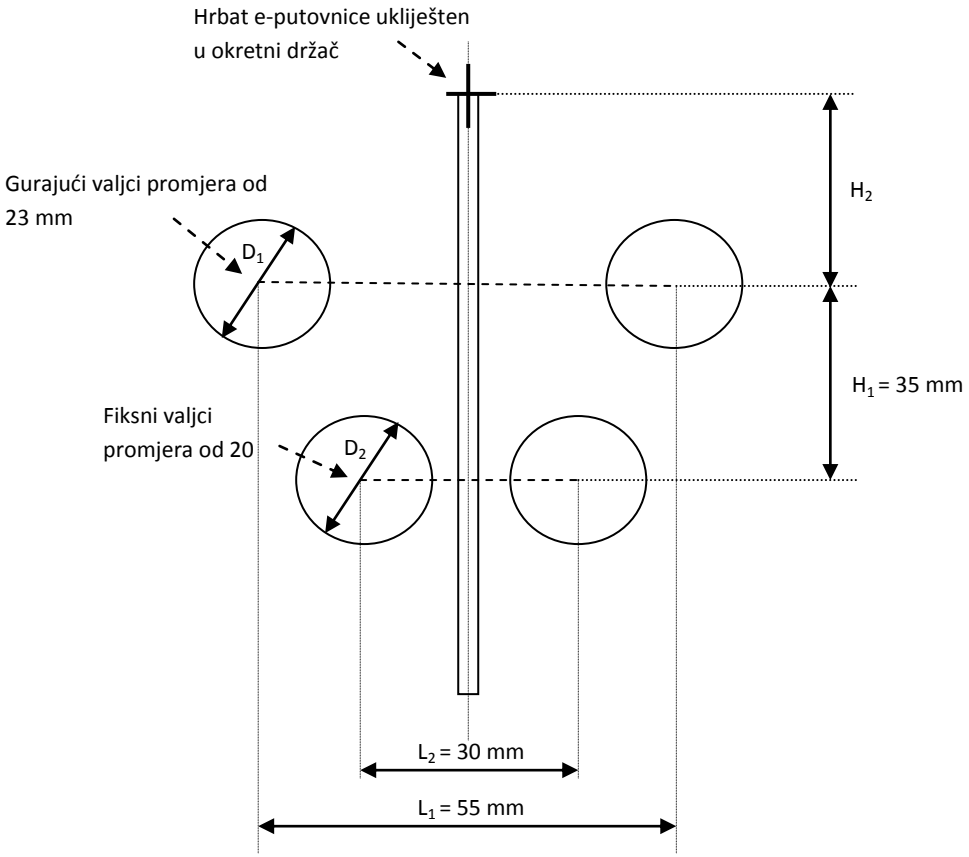
n = broj ciklusa savijanja putovnica

0 = orijentacija knjižice u uređaju

Izlazni parametri

Nema ih.

Karakteristike testa dinamičnog savijanja



Slika 65 - Skica sustava gurajućih i fiksnih valjaka – početna pozicija

- gurajući valjci su namješteni tako da osiguravaju jednaki otklon e-putovnice od centralne pozicije u svakom taktu.
- Udaljenost H2 između ukliještenog hrpta e-putovnice i centra gurajućih valjaka je podesiva između 40 i 58 mm
- Gurajući valjci i fiksni valjci su udaljeni od centra do centra za 35 mm (H1)
- Gurajući valjci imaju vanjski promjer od 23 mm (D1) i međusobno su udaljeni za 55 mm (L1) od centra do centra.
- Fiskni rotirajući valjci su međusobno udaljeni od centra do centra za 30 mm (L2) i imaju vanjski promjer od 20 mm (D2).

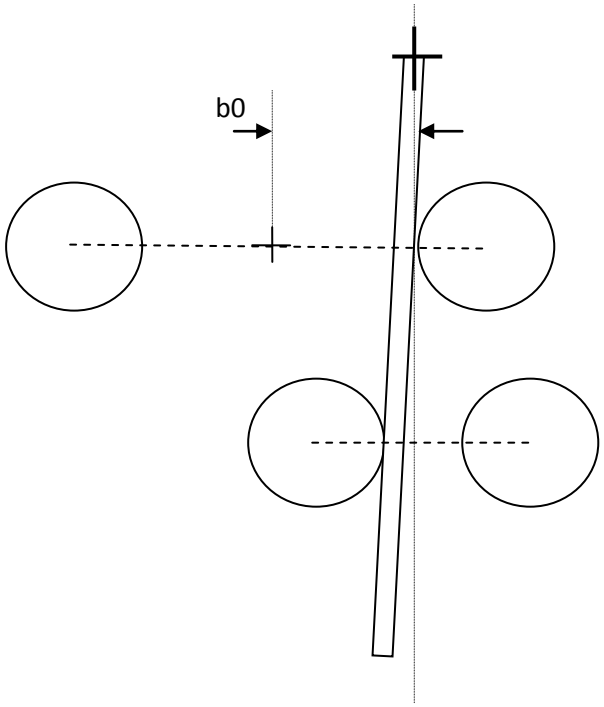
Kalibracija

- Prije početka testiranja uređaj je potrebno kalibrirati. Za kalibraciju uređaja korištena je zasebna putovnica, specifično određena za postupak kalibracije.

- Uzimajući u obzir orijentaciju e-putovnice (O), e-putovnica je ukliještena na jednom kraju i slobodno se pomiče na drugom kraju. Orijentacija sve 4 e-putovnice u uređaju je ista, tj. podešena je u smjeru glava – noge.

- Udaljenost H2 podešena je na 40 mm.

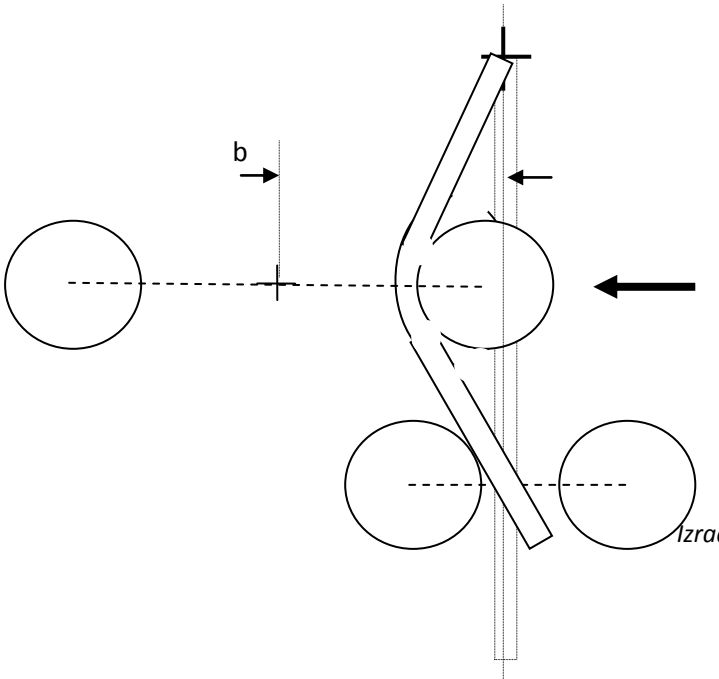
- Gurajući valjci se u postupku kalibracije pomiču tako da guraju knjižicu o fiksne valjke bez savijanja putovnice kao što je prikazano na slici 2. Iznos pomicanja valjka je b0 i predstavlja inicijalnu poziciju.



Slika 66 - Inicijalna pozicija gurajućih valjaka

Način testiranja

- Maksimalni put gurajućih valjaka je b0 + 20 mm. Nakon postavljanja inicijalne pozicije primijenjena je sila od 40 N u smjeru deblje strelice na slici 3 u trajanju od 1 minute.



Slika 67 – Skica savijanja

Izradila: Željka Stražnicky, lipanj 2011.

- Automatski je zabilježen maksimalni put gurajućih valjaka na ± b.
- Podešena frekvencija savijanja je 0,5 Hz za n savijanja.
- Jedan ciklus savijanja predstavlja savijanje u oba smjera.

Slika 68 – Slika testiranja putovnica metodom dinamičnog savijanja (izvor: AKD)

11.9.2. Test torzijskog zamora putovnice - Torsion stress

Svrha

Svrha ovog testa je odrediti nepovoljan mehanički ili funkcionalni efekt kod e-putovnica koji proizlazi iz torzijskog zamora.

Uređaj za testiranje

Korišteni uređaj za testiranje dinamičkog savijanja putovnica je **PPT 2007/T** proizvođača Muehlbauer AG (Njemačka). U uređaj se istovremeno mogu smjestiti maksimalno 4 putovnice.

Karakteristike uređaja

Visina:	280 mm
Širina:	552 mm
Dubina:	593 mm
Težina:	cca. 38 kg
Napon:	230 V
Snaga:	250 W
Jačina struje:	6 A
Jačina zvuka:	max. 55,1 dB (A)

Tablica 29 – Karakteristike uređaja PPT 2007/T

Testni preduvjeti

Temperatura okoline:	23˚C ± 5˚ C
Relativna vlažnost:	40 % - 60 %

Tablica 30 – Testni preduvjeti

Ulazni parametri

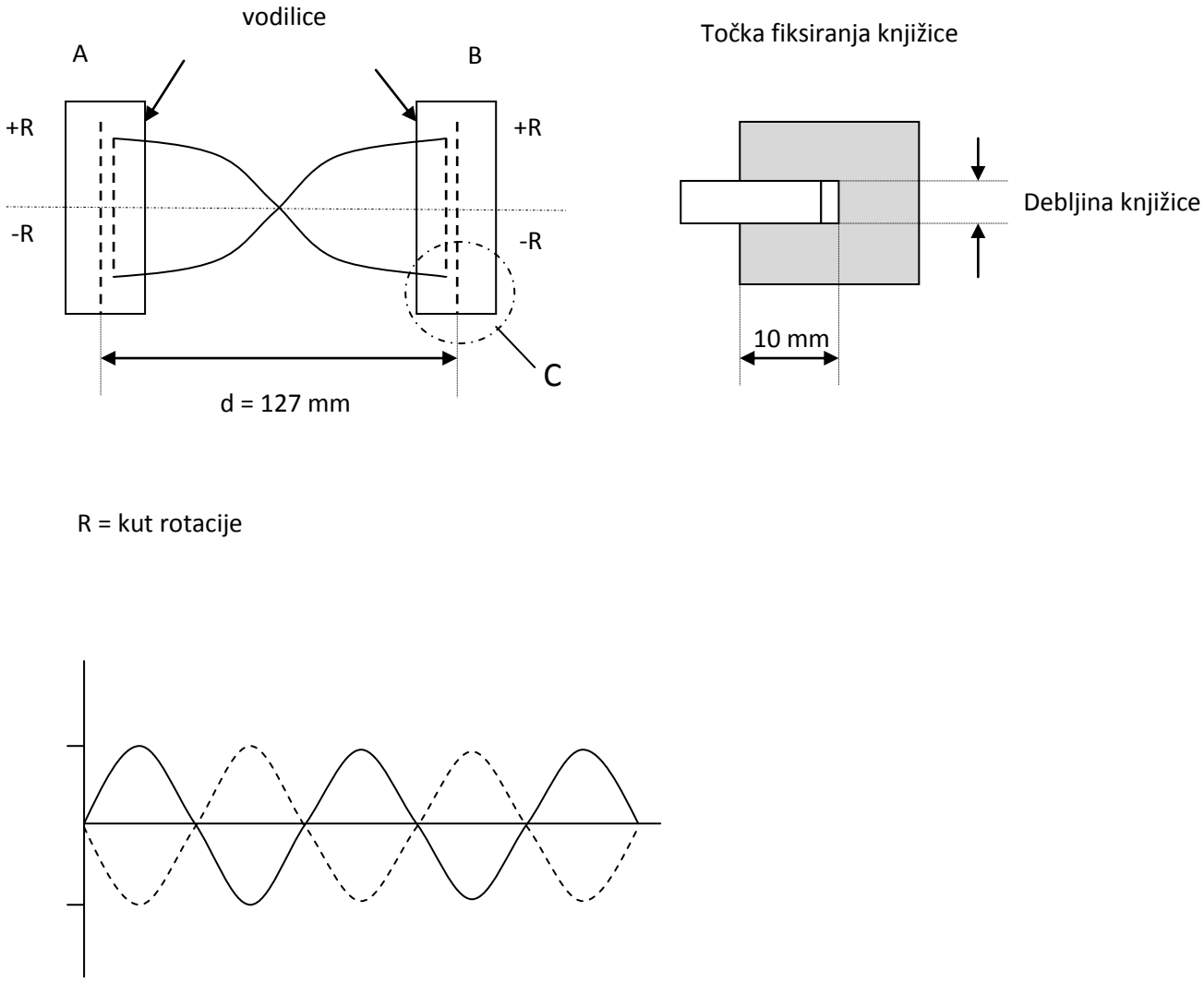
n = broj ciklusa torzije putovnica

Izlazni parametri

Nema ih.

Karakteristike testa torzijskog zamora

Testni uređaj primjenjuje torzijski pokret kako je to prikazano na slici 4.



Slika 69 - Skica uređaja i pripadajućeg torzijskog gibanja

Kalibracija

- Vodilice se otvore te se u njih položi knjižica putovnice. Vodilice drže putovnicu u glavi i nogama.
- Kut zakreta vodilica je podešen na 15 ˚.

- Primijenjen je moment sile od 0,3 N-m u trajanju od 1 min.
- Za kalibraciju uređaja korištena je zasebna putovnica, specifično određena za postupak kalibracije.

Način testiranja

- Sve 4 knjižice e-putovnice se smjeste u uređaj, a vodilice se fiksiraju.
- Jedan ciklus se sastoji od slijedećih kontinuiranih koraka:
    - Početna je pozicija ondje gdje su vodilice A i B pri kutu od 0˚.
    - Vodilica A se rotira na kut +R, dok se simultano vodilica B rotira na kut –R
    - Vodilica A se rotira na kut 0˚, dok se simultano vodilica B isto tako rotira na kut 0˚
- Podešena frekvencija torzije je 0,5 Hz za n ciklusa.

Slika 70 – Slika testiranja putovnica metodom torzijskog zamora (izvor: AKD)

11.9.3. Test djelovanja silom - Impact stress

Svrha

Svrha ovog testa je primijeniti definiranu silu na knjižicu e-putovnice kako bi se simuliralo pečatiranje dokumenta na graničnim prijelazima.

Uređaj za testiranje

Korišteni uređaj za testiranje dinamičkog savijanja putovnica je **PPT 2007/I** proizvođača Muehlbauer AG (Njemačka). U uređaj se istovremeno može smjestiti maksimalno 1 putovnica.

Karakteristike uređaja

Visina:	280 mm
Širina:	552 mm
Dubina:	593 mm
Težina:	cca. 38,4 kg
Napon:	230 V
Snaga:	250 W
Jačina struje:	6 A
Jačina zvuka:	max. 55 dB (A)

Tablica 31 – Karakteristike uređaja PPT 2007/I

Testni preduvjeti

Temperatura okoline:	23˚C ± 5˚ C
Relativna vlažnost:	40 % - 60 %

Tablica 32 – Testni preduvjeti

Ulazni parametri

S = stranica putovnice koja je izložena djelovanju sile. Kako su samo VISA stranice u knjižici putovnice izložene pečatiranju na graničnim prijelazima, potrebno je najbližu VISA stranicu okrenuti preko stranice koja se želi izložiti djelovanju sile. Stranica na koju se želi djelovati silom je ili PC stranica ili zadnja stranica korica.

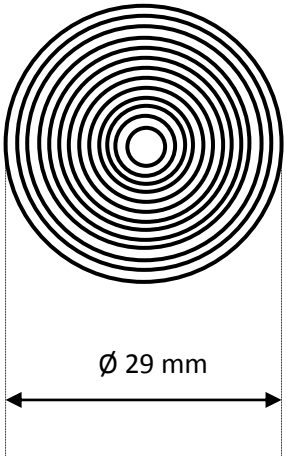
Izlazni parametri

Nema ih.

Karakteristike testa torzijskog zamora

Pečat

- Lice pečata je ravna čvrsta podloga od čelika, promjera od 29 mm.
- Na površini lica pečata su jetkani koncentrični krugovi.
- Profil krugova je četvrtast, sa minimalnom dubinom od 0,3 mm, Širina krugova je 1mm ± 0,1 mm, a nominalna udaljenost između krugova je 1,5 mm.
- Nominalni promjer centralnog kruga je 1 mm.
- Akumulirana tolerancija udaljenosti krugova je ± 0,5 mm.



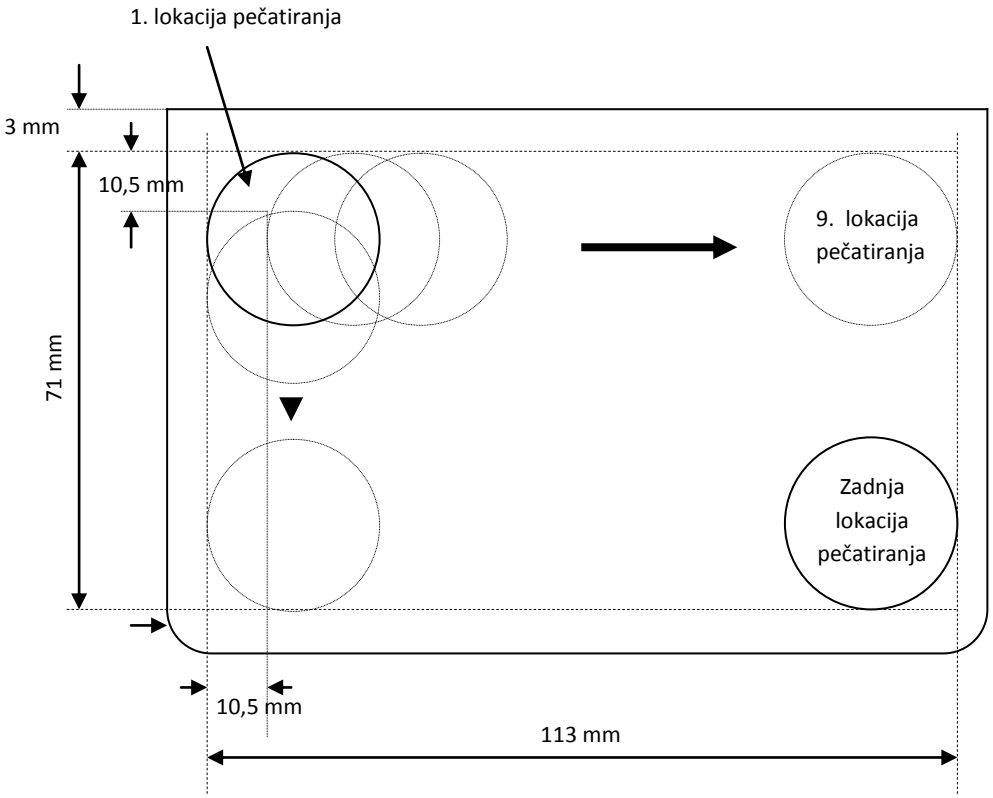
Slika 71 - Uzorak udarca uzrokovan strukturom pečata

- Pečat je izrađen na način da se sastoji od čelika iz jednog dijela mase M
- U uređaju postoje vodilice pečata koje pečat podižu i spuštaju ga da padne na podlogu silom slobodnog pada.
- H = nominalna visina (mm) sa koje je pečat pušten na dokument ili težina koja je puštena na dokument, čime se udarna brzina određuje prema formuli ubrzanja inertnih tijela pod Zemljinom gravitacijom.
- H je između 0,05 m i 0,20 m.
- M = težina (kg) pečata
- D = pomak između dva udarca

Način testiranja

- Potrebno je odrediti stranicu S koja je ili PC stranica ili zadnji dio korica putovnice (ovisno o poziciji čipa u putovnici).

- Potrebno je odrediti najbližu VISA stranicu koja može biti pečatirana te ju okrenuti iznad stranice S.
- Putovnica se otvori za 180˚ i položi na ravnu podlogu uređaja koja je prekrivena gumenom navlakom. Podloga fiksira putovnicu pomoću držača u glavi i nogama.
- Pečat mase M se pušta sa visine H na svaku lokaciju na dokument kako je prikazano na slici 6. Pečat se pomiče od prve do zadnje lokacije od lijeva prema desnoj strani i odozgo prema dolje.
- Budući da se u uređaj može smjestiti maksimalno 1 putovnica, postupak je potrebno ponoviti za sve putovnice koje su definirane testom.



Slika 72 – Lokacije udaranja pečata

11.10. Test funkcionalnosti beskontaktnog čipa

Svrha

Utvrditi ispravnost čipa nakon izloženosti e-putovnica metodama testiranja mehaničkog utjecaja.

Uređaj za testiranje

Korišteni hardver za testiranje je beskontaktni čitač Omnikex Cardman 5321 spojen putem USB ulaza na osobno računalo koji komunicira prema definiranom standardu za

beskontaktna sučelja ISO/IEC 14443. Korišteni softver za očitanje valjanosti čipa je Eclipse, instaliran na osobno računalo.

Način testiranja

Po završetku pojedinog kruga testiranja svaku pojedinačnu putovnicu se prislonilo na beskontaktni čitač te u aplikaciji Eclipse zadala naredba /ATR. ATR (*Answer to reset*) je sekvenca povratnih byte-ova od strane čipa koji se generiraju nakon što je čitač uspostavio električku komunikaciju s čipom.

11.11. Rezultati testiranja

PUTOVNICA A							
	BROJ PONAVLJANJA PO TESTU				REZULTAT (OK/NOK)		
	DB	**T**	**I**	PROVJERA FUNKCIONALNOSTI ČIPA	**DB**	**T**	**I**
I. KRUG	1000	500	4	DA	**OK**	**OK**	**OK**
II. KRUG	2000	1000	8	DA	**OK**	**OK**	**OK**
III. KRUG	4000	2000	16	DA	**OK**	**OK**	**OK**
IV. KRUG	8000	4000	32	DA	**OK**	**OK**	**OK**
V. KRUG	16000	8000	64	DA	**OK**	**OK**	**OK**

Tablica 33 – Rezultati testiranja putovnice proizvođača A

PUTOVNICA B							
	BROJ PONAVLJANJA PO TESTU				REZULTAT (OK/NOK)		
	DB	**T**	**I**	PROVJERA FUNKCIONALNOSTI ČIPA	**DB**	**T**	**I**
I. KRUG	1000	500	4	DA	**OK**	**OK**	**OK**
II. KRUG	2000	1000	8	DA	**OK**	**OK**	**OK**
III. KRUG	4000	2000	16	DA	**OK**	**OK**	**OK**
IV. KRUG	8000	4000	32	DA	**OK**	**OK**	**OK**
V. KRUG	16000	8000	64	DA	**OK**	**OK**	**OK**

Tablica 34 – Rezultati testiranja putovnice proizvođača B

PUTOVNICA C							
	BROJ PONAVLJANJA PO TESTU				REZULTAT (OK/NOK)		
	DB	**T**	**I**	PROVJERA FUNKCIONALNOSTI ČIPA	**DB**	**T**	**I**
I. KRUG	1000	500	4	DA	**OK**	**OK**	**OK**
II. KRUG	2000	1000	8	DA	**OK**	**OK**	**OK**
III. KRUG	4000	2000	16	DA	**OK**	**OK**	**OK**
IV. KRUG	8000	4000	32	DA	**OK**	**OK**	**OK**
V. KRUG	16000	8000	64	DA	**OK**	**OK**	**OK**

Tablica 35 – Rezultati testiranja putovnice proizvođača C

PUTOVNICA D							
	BROJ PONAVLJANJA PO TESTU				REZULTAT (OK / NOK)		
	DB	**T**	**I**	PROVJERA FUNKCIONALNOSTI ČIPA	**DB**	**T**	**I**
I. KRUG	1000	500	4	DA	**OK**	**OK**	**OK**
II. KRUG	2000	1000	8	DA	**OK**	**OK**	**OK**
III. KRUG	4000	2000	16	DA	**OK**	**OK**	**OK**
IV. KRUG	8000	4000	32	DA	**OK**	**OK**	**OK**
V. KRUG	16000	8000	64	DA	**OK**	**OK**	**OK**

Tablica 36 – Rezultati testiranja putovnice proizvođača D

12. ZAKLJUČAK

Rezultat istraživanja magistarskog rada pokazao je uniformnost u kvaliteti medija za smještaj čipa svih ispitivanih putovnica, promatranu sa aspekta funkcionalnosti čipa nakon primijenjenih metoda testiranja usklađenih sa referentnim standardom [32].

Kao donja granica ispitivanja kvalitete postavljena je vrijednost definirana standardom, a ista je postupno povećavana 16 puta kako bi se eventualno utvrdila granica probijanja kvalitete očitovane kroz ispravnost/ne-ispravnost čipa. Ispravnost čipa provjeravana je nakon svake nove postavljene razine kvalitete definirane brojem ponavljanja mehaničke radnje pojedinog testa, provjerom ATR (*answer to reset*) funkcionalnosti. Kod oba tipa e-putovnica (sa e-koricama i PC identifikacijskim stranicama) svih ispitivanih proizvođača, rezultat ispitivanja je identičan, dakle pozitivan. Ispitani čipovi svih putovnica pokazali su identične, pozitivne rezultate.

Kako su ispitivanja trajala kontinuirano 2 mjeseca, postavljena gornja granica, odnosno broj ponavljanja po metodi, nije dalje povećavan. Razlog tome je vremenska komponenta koja bi time bila najmanje udvostručena, odnosno ukupno vrijeme testiranja značajno produženo, te pretpostavke da daljnje povećanje broja ponavljanja ne bi znatno promijenilo rezultat. Korištena oprema koncipirana je na način da ne dozvoljava promjenu ritma rada, u smislu ubrzanja i skraćenja vremena testiranja, kao niti promjenu ostalih pred-definiranih postavki vezanih uz fizikalne parametre, poput sile pečatiranja, frekvencije rada i sl.

Navedena ispitivanja mogu se produbiti primjenom kompleksnijih metoda analize utjecaja testiranja na električke karakteristike sustava čip – antena, za što je neophodno dodatno istraživanje materije povezane s elektrotehničkim svojstvima beskontaktne komunikacije te primjena metoda testiranja razine 1-4, ICAO standarda – *ICAO TR: RF Protocol and Application Test Standard for E- passport – part 2; version 1.02, 2007*. Međutim, ovaj magistarski rad isključivo je koncentriran na testiranja definirana ICAO standardom „*Durability of Machine Readable Passports*“ [31].

Dobiveni uniformni rezultat ispitivanja nudi objašnjenje zašto su se na tržištu, jednakom mjerom i u jednakoj razini kvalitete izrade, profilirali i proizvođači e-korica i proizvođači PC identifikacijskih stranica. TIme nije moguće utvrditi koje od ova 2 rješenja čini kvalitetnije sa aspekta očuvanja čipa od mehaničkih utjecaja. Prave rezultate vezane uz izdržljivost e-putovnica pokazati će tijek vremena životnog vijeka dokumenta od 10 god. i njegove uporabe na tržištu. Da li je donja razina kvalitete postavljena od strane ICAO-a preniska i hoće li se dodatno povećati radi pomicanja granice očekivane kvalitete novim proizvođačima i proizvodima pokazati će narednih nekoliko godina.

Evidentno je kako odabir jedno od ova 2 rješenja smještaja čipa u e-putovnici ne može biti temeljen isključivo na dobivenim rezultatima ispitivanja. Konačni odabir rješenja stoga mora proizaći iz analize više različitih aspekata koji determiniraju:

- dodanu vrijednost novom proizvodu,
- očuvanost/tehničko stanje postojeće opreme za personalizaciju,
- suvremenost tehnologije personalizacije,
- mogućnost ili potrebu za optimizacijom ukupnog proizvodnog procesa izrade putovnica,
- buduće strateške ciljeve tvrtke,
- utjecaj na konačnu cijenu izrade i personalizacije.

Prednost između ova 2 rješenja u projektu „*Biometrijska e-putovnica hrvatskih državljana*“ u Republici Hrvatskoj dana je smještaju čipa unutar PC identifikacijske stranice. Razlozi za takvu odluku proizlaze iz kombinacije gore navedenih aspekata.

13. LITERATURA

1) www.passport.gc.ca/pptc/hist.aspx?lang=eng
2) http://apostille.us/news/the_passport_the_history_of_mans_most_travelled_document.sh.
3) „**ICAO Civil Aviation and MRTD Standards**“// Keesing Journal of Documents & Identity, issue 31, 2010
4) http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx
5) „**Results ICAO April 2010 deadline**“// Keesing Journal of Documents & Identity, Annual Report 2010-2011
6) „**Pamet u putovnicama**“// Zaštita, časopis za zaštitu i sigurnost osoblja i imovine, broj 1, ožujak 2010.
7) Machine Readable Travel Documents, Part 1, Volume 1, **Passports with Machine Readable Data Stored in Optical Character Recognition Format**, sixth edition, 2006
8) **Council Regulation (EC) No. 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States**
9) „**Identity management & travel documents**“//Keesing Journal of Documents & Identity, issue 25, 2008
10) Machine Readable Travel Documents, Part 1, Volume 2, **Specifications for Electronically Enabled Passports with Biometric Identification Capabilities**, sixth edition, 2006
11) http://www.smartcardalliance.org/resources/pdf/contactless_business_benefits.pdf
12) „**Implementation of PKI Enabled Digital Signatures for MRTDs**“// ICAO/TAG Technical Report, April 19, 2003
13) http://www.ibm.com/developerworks/library/s-crypt03.html
14) http://www.docstoc.com/docs/32528785/SEMINARSKI-RAD-INFRASTRUKTURA-JAVNOG-KLJU%C4%8CA-PKI-%E2%80%93-Public-Key
15) „**PKI for Machine Readable Travel Documents offering ICC Read-Only Acces**“// ICAO/TAG Technical Report, Version 1.1, October 2004.
16) **Machine Readable Travel Documents – Extended Access Control (EAC)** // Federal office for information security, Version 2.0 Public Beta 1, lipanj 2007
17) PKD Board Annual Report 2010
18) PKD Fee Schedule 2011
19) http://prado.consilium.europa.eu/EN/homeIndex.html
20) „**The future: A vision**“ // MRTD Report – Volume 5 - Number 1 – 2010

Izradila: Željka Stražnicky, lipanj 2011.

21) Roderick Heitmeyer; „**ICAO Civil Aviation and MRTD Standards**“ // Keesing Journal of Documents & Identity, Issue 31, 2010

22) „**The e-Passport – Transition from the first to second generation**“ // Keesing Journal of Documents & Identity, Annual Report ePassports, 2009 - 2010

23) „**2010 Deadline – Machine readable Passport**“ // Keesing Journal of Documents & Identity, Annual Report ePassports, 2009 - 2010

24) „**The e-passport industry – Past, present and future**“ // Keesing Journal of Documents & Identity, Annual Report ePassports 2008 - 2009

25) David Landsman (De La Rue Identity Systems) „**Identity management & travel documents**“ // Keesing Journal of Documents & Identity, Issue 25, 2008

26) Malcolm Cuthbertson (De La Rue Identity Systems); „**Passports – the state of play**“ // Infosecura, Number 36, July 2008

27) Allan Harle (Inspectron Holding plc); „**Electronic security documents**“ // The silicon Trust Report, Issue 2, 2007

28) „**Borderless Europe**“ // Infosecura; Number 34, December 2007

29) Paul De Hert, Wim Schreurs&Evelien Brouwer; „**Machine – readable identity documents with biometric data in the EU – part IV**“ // Keesing Journal of Documents & Identity, Issue 24, 2007

30) Jan van den Berg (SDU Identification); „**Testing three types of e-passports**“ // Keesing Journal of Documents & Identity, Issue 8, 2004

31) „**Durability of Machine Readable Passports**“ // ICAO, Machine Readable Travel Documents, Technical Report version: 3.2, date: 2006-08-30

32) „**Specifications for Electronically Enabled Passports with Biometric Identification Capability**“ // ICAO, Machine Readable Travel Documents, Part 1, Machine Readable Passports, Volume 2, sixth edition, 2006

33) **EU council No. C 179/1**, Sumplementary resolution tothe resolution adopted on 23 June 1981 concerning the adoption of a passport of uniform pattern, of the representatives oft he Governments oft he Member States oft he European Communities, meeting within the Council on 30 June 1982

34) Jörg Fischer (Bundesdruckerei); **„Innovative display technologies for future ID documents“** // ID Credentials, The Journal of secure identity solutions, 2010

35) http://www.fime.com/durabilitytesting/128755.shtml

36) Yahya Haghiri, Thomas Tarantino; „ **Smart Card Manufacturing, a Practical Guide**“ // Giesecke and Devrient GmbH, Munich, Germany, 1999

ŽIVOTOPIS

Rođena 21. travnja 1977. u Vinkovcima (Republika Hrvatska). Osnovnu školu „Moša Pijade“ pohađa u Županji, a srednju prirodoslovno-matematičku gimnaziju „Matija Antun Reljković“ u Vinkovcima. Po završetku srednje škole upisuje Grafički fakultet u Zagrebu (šk.god. 1995./96.), a diplomira krajem 2001. god. na katedri za fiziku u grafičkoj tehnologiji sa temom diplomskog rada „Utjecaj UV zračenja na optička svojstva četverobojnih ofsetnih tiskovnih podloga“, pod vodstvom mentora Mr.sc. Višnje Mikac Dadić.

2002. god. zapošljava se u tvrtki Agencija za komercijalnu djelatnost d.o.o. u Zagrebu gdje radi do današnjih dana. Protekom pripravničkog staža u trajanju od jedne godine biva razmještena u organizacijsku jedinicu Kontrole kvalitete na radno mjesto Kontrolor tehnološkog procesa. U navedenoj org. jedinici radi do 2004. god. kada postaje dijelom mladog tima „istraživača“ u novo oformljenoj organizacijskoj jedinici Istraživanje i razvoj. U Istraživanju i razvoju radi i danas, a kroz godine rada napreduje od radnog mjesta voditelj projekta, preko stručnog suradnika za razvoj pametnih kartica do voditelja org. jedinice istraživanje i razvoj na kojem se zadržava od 2009. god. U međuvremenu upisuje magistarski studij, smjer Grafičko inženjerstvo na Grafičkom fakultetu.

Pohađa brojne stručne domaće i inozemne konferencije i seminare sa specijalizacijom na temu zaštitnog tiska i zaštitnih elemenata u proizvodnji dokumenata, proizvodnje polimernih (plastičnih) kartica kao novog smjera u industriji izrade dokumenata i zaštitnih tiskovina te sudjeluje u brojnim projektima izrade „pametnih“ kartica na području Republike Hrvatske. Također učestvuje i u projektima odabira, nabavke i implementacije novih tehnologija u poslovne procese AKD-a, među kojima je i tehnologija izrade polimernih kartica ID1 formata velikih kapaciteta, koja obuhvaća proizvodne procese tiska, izrade tijela kartice, dorade i personalizacije, te koja postaje novi značajni proizvodni i prodajni segment AKD-a na domaćem i inozemnom tržištu.

U svom radu specijalizira se u segmentu proizvodnje i personalizacije polimernih kartica te elektroničkih dokumenata i pratećih sustava sa primjenom projektne metodologije rada.

2009. god. biva član projekta izrade biometrijske e-putovnice hrvatskih državljana sa ulogom tehničkog koordinatora ispred AKD-a.

Izradila: Željka Stražnicky, lipanj 2011.