

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

OCENA STANJA IN VARNOSTI INFORMACIJSKIH SISTEMOV OVERJANJA
IDENTITETE PRI UPORABI POTOVALNIH DOKUMENTOV Z BIOMETRIČNIMI
PODATKI

Ljubljana, maj 2009

ŽELJKO LALIČ

IZJAVA

Študent Željko Lalić izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Borke Jerman Blažič, in da dovolim njegovo objavo na fakultetnih spletnih straneh.

V Ljubljani, dne 27.05.2009

Podpis: _____

KAZALO

KAZALO	i
Uvod	1
1 Biometrija.....	1
1.1 Opredelitev biometrije	1
1.2 Biometrične metode	2
1.2.1 Vpis in potek prepoznavne biometričnih podatkov	3
1.3 Zmogljivost biometričnih sistemov.....	4
1.4 Trendi v biometriji	5
1.5 Standardi in zakonodaja	6
2 Informacijski sistemi	6
2.1 Splošno o informacijskih sistemih	6
2.2 Schengenski informacijski sistem	6
2.2.1 Schengen	6
2.2.2 Schengenski pravni red	9
2.2.3 Schengenski informacijski sistem	10
2.2.4 SIS I+	14
2.2.5 SIS II	14
2.2.6 Uvajanje schengenskega sistema v Sloveniji.....	18
2.2.7 Schengen in sredstva EU.....	22
2.2.8 Stroški SIS.....	22
2.2.9 Zgodovina Schengenskega sporazuma.....	23
2.3 Pruemaska pogodba (SIS III).....	24
2.4 Vizumski informacijski sistem (VIS).....	25
2.5 Eurodac.....	26
2.6 Next Generation Identification.....	26
3 Biometrični potovalni dokumenti.....	27
3.1 Skladnost s standardi.....	28
3.2 Slovenski potni list.....	29
3.2.1 Čip.....	29
3.2.2 Podatki na čipu	30
3.2.3 Zaščita podatkov na čipu.....	31
3.2.4 Ponarejanje biometričnih potnih listov	33
3.3 Vrste potnih listov	38
Sklep.....	39
Literatura in viri	40

KAZALO SLIK

Slika 1: Vpis biometričnih podatkov.....	3
Slika 2: Potek prepoznavne.....	4
Slika 3: Letni prihodki v biometrični industriji v obdobju 2007–2015 (v milijardah USD)	5
Slika 4: Tržni deleži po regijah v letih 2007 in 2015	5

KAZALO TABEL

Tabela 1: Primerjava različnih biometričnih podatkov in njihova uporabnost za razpoznavanje identitete.....	3
Tabela 2: Časovni pregled integracije.....	8
Tabela 3: Podatki o večletnih odobrenih izdatkih za postavitev tehnične podporne funkcije C.SIS	23
Tabela 4: Predvideni stroški postavitve in obratovanja sistema C.SIS v letih 2008 in 2009 (v EUR).....	23

Uvod

Razvoj biometričnih potnih listov se je začel sredi 80-ih let prejšnjega stoletja. Potni listi, ki bi vsebovali določene biometrične lastnosti lastnika, bi onemogočili ali pa vsaj otežili njihovo ponarejanje. Po prvotnih načrtih naj bi vse države, ki so članice Mednarodne organizacije za civilno letalstvo, z izdajanjem biometričnih potnih listov začele najpozneje do leta 2010, vendar se je uvajanje biometrije v potne liste pospešilo po terorističnih napadih v ZDA 11. septembra 2001.

Po napadih so v ZDA uvedli strožje varnostne zahteve. Med drugim so začeli zbirati biometrične podatke vseh oseb, ki za vstop v ZDA potrebujejo vizum. Za države, katerih državljani ne potrebujejo vizuma za obisk ZDA (države, ki so podpisale program za opustitev viz – Wisa Waiver Program), pa so bili uvedeni drugačni ukrepi. Najpozneje do 26. oktobra 2006 so bile te države primorane začeti izdajati biometrične potne liste, saj bi bili v nasprotnem primeru zanje ponovno uvedeni vizumi.

Z vključitvijo biometričnih podatkov naj bi dobili zanesljivejše potne liste, ki so bolj učinkoviti pri identifikaciji, obenem pa jih je tudi težje ponarediti. Namen pričujočega diplomskega dela je z informacijskega in varnostnega vidika ugotoviti stanje in uporabnost biometričnih podatkov v e-upravi s poudarkom na potovalnih dokumentih.

Diplomsko delo je razdeljeno na tri poglavja. V prvem sem opredelil biometrijo in biometrične metode. V drugem poglavju sem se osredotočil na informacijske sisteme. Poudarek je na Schengenskem informacijskem sistemu prve in druge generacije, poglavje pa sem zaključil še z drugimi primeri informacijskih sistemov. V zadnjem poglavju sem predstavil biometrične potovalne dokumente, predvsem slovenski potni list oz. potni list EU. Na koncu poglavja sem podal še primere ponarejanja potnih listov ter vrste potnih listov, ki jih poznamo v Sloveniji.

1 Biometrija

1.1 Opredelitev biometrije

Pojem biometrija (tudi biometrika) se nanaša na dve različni področji.

Prvotno je bila biometrija veja biologije, ki preučuje biološka in biomedicinska vprašanja z uporabo matematično-statističnih metod (Slovenski veliki leksikon 1: A–G, 2003, str. 202).

Čedalje bolj pa se biometrija uveljavlja kot veda o načinih prepoznavne ljudi na podlagi njihovih telesnih in vedenjskih značilnosti, ki jih imajo vsi posamezniki, so edinstvene in stalne za vsakega posameznika posebej in s katerimi je možno posameznika tudi določiti (*Biometrija*, 2009a, informacijski pooblaščenec).

V informacijski tehnologiji se biometrija nanaša na proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih in vedenjskih lastnostih z namenom identifikacije in avtentikacije, zlasti v e-poslovanju in e-upravi (*Biometrija*, 2009b, Wikipedija, prosta enciklopedija).

1.2 Biometrične metode

Poleg biometrije poznamo tudi druge načine ugotavljanja oz. preverjanja identitete. Prva skupina temelji na »tistem, kar oseba ima« (npr. bančna kartica), druga skupina pa na »tistem, kar oseba ve« (osebno geslo, PIN koda). Biometrija sodi v tretjo skupino, ki temelji na »tistem, kar oseba je«.

Kot taka ima biometrija pred ostalima načinoma velike prednosti. Kar posedujemo, lahko izgubimo ali nam ukradejo, gesla se pozabijo ali razkrijejo, biometrične značilnosti pa načeloma ostanejo večne, ne morejo se izgubiti ali pozabiti, težko jih je ponarediti oziroma prenesti na drugo osebo. Najzanesljivejša je kombinacija vseh treh načinov.

Biometrična značilnost je tista lastnost oz. značilnost posameznika, ki je merljiva in s pomočjo katere lahko posameznika tudi določimo.

Ločimo jih na:

- telesne (podoba obraza, prstni odtis, šarenica, mrežnica, dlan, uhelj, preplet ven na roki, DNK ...),
- vedenjske (lastnoročno podpisovanje, glas, gibanje, tipkanje).

Niso pa vse človeške značilnosti enako primerne za uporabo v biometriji. Da je neka značilnost primerna, morajo biti izpolnjeni določeni pogoji:

- univerzalnost – vsaka oseba mora imeti tako značilnost,
- edinstvenost – niti dve osebi ne smeta imeti enake značilnosti,
- stalnost – značilnost se s staranjem osebe ne sme spreminjati,
- merljivost – zajem podatkov mora biti enostaven,
- sprejemljivost – metoda mora biti uporabniku prijazna.

V tabeli 1 je navedeno, kako biometrične značilnosti ustrezajo določenim kriterijem. Značilnosti, ki imajo več zvezdic, bolj ustrezajo določenemu pogoju.

Tabela 1: Primerjava različnih biometričnih podatkov in njihova uporabnost za razpoznavanje identitete

	Univerzalnos t	Edinstvenost	Stalnost	Merljivost	Sprejemljivost
Prstni odtis	**	***	***	**	**
Podoba obraza	***	*	**	***	***
Geometrija roke	**	**	**	***	**
Šarenica	***	***	***	**	*
Glas	**	*	*	**	***
DNK	***	***	***	*	*
Mrežnica	***	***	**	*	*
Tipkanje	*	*	*	**	**
Podpis	*	*	*	***	***
Preplet ven	**	**	**	**	**
Vonj	***	***	***	*	**

Vir: Biometrics, 2009, Wikipedia, The Free Encyclopedia

1.2.1 Vpis in potek prepoznave biometričnih podatkov

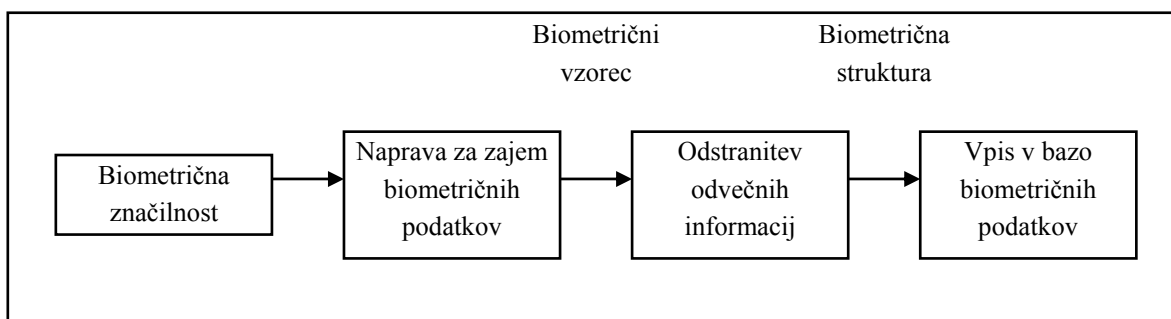
Biometrični sistemi lahko opravljajo dve funkciji, in sicer verifikacijo ter identifikacijo.

Pri verifikaciji gre za preverjanje, ali je uporabnik res tista oseba, za katero se predstavlja – gre za primerjavo 1:1. Zaradi tega je proces verifikacije zelo hiter.

Pri identifikaciji pa je proces bolj zahteven, saj gre za določanje osebe, kar pomeni primerjavo 1:n.

Da bi s pomočjo biometrije prepoznali določeno osebo, je za vsako osebo najprej potreben vpis biometričnih podatkov v njihovo bazo. Baza podatkov poleg biometričnih vsebuje tudi druge podatke, kot so npr. ime, priimek, osebna številka ... Potek vpisa je prikazan na sliki 1.

Slika 1: Vpis biometričnih podatkov



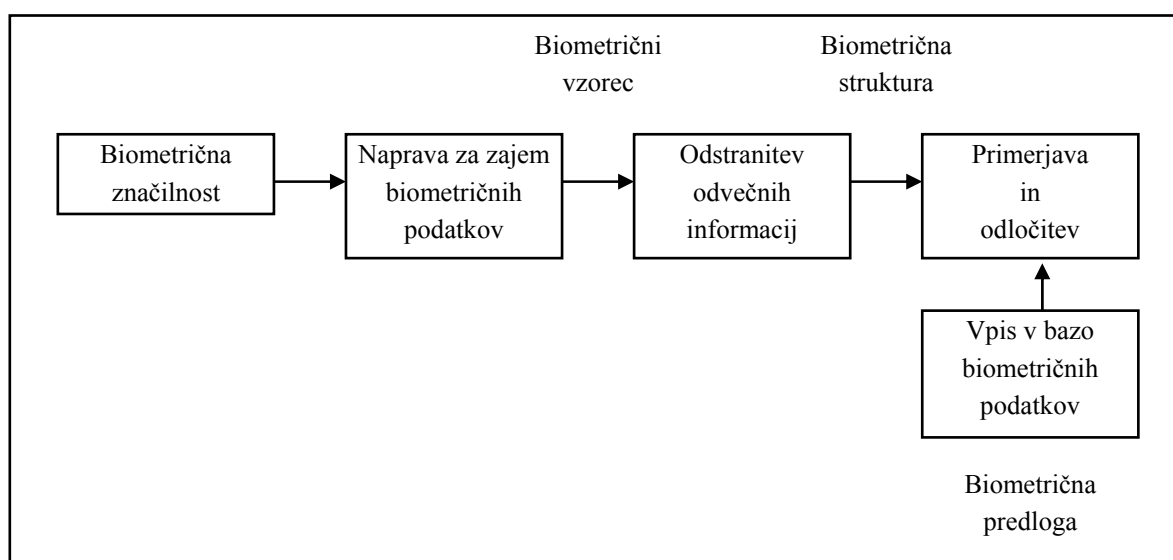
Vir: Bioidentification, 2009

Analogni ali digitalni podobi biometričnih značilnosti rečemo biometrični vzorec. Dobimo ga z napravo za zajem biometričnih podatkov. Ker vzorec pogosto vsebuje več informacij, kot

jih je potrebno za prepoznavo osebe, se vse odvečne informacije odstranijo, kar pripomore k hitrejši prepoznavi. Skupek informacij, ki so lahko uporabne za prepoznavo, se shrani kot biometrična predloga.

V postopku prepoznave oseba v napravo za zajem biometričnih podatkov vnese zahtevano biometrično značilnost. Naprava ustvari biometrični vzorec, iz katerega odstrani odvečne informacije. Na ta način dobljeno, t. i. biometrično strukturo, potem primerja z eno ali več biometrijskimi predlogami iz baze podatkov. Potek prepoznave je prikazan na sliki 2.

Slika 2: Potek prepoznave



Vir: Bioidentification, 2009

1.3 Zmožljivost biometričnih sistemov

Biometrične metode imajo tudi omejitve. Pri kontroli dostopa imamo na primer dve vrsti uporabnikov, t. i. stranke (uporabnike) in vsiljivce. Tako sta možni dve napaki – dostop je lahko zavrnjen stranki (uporabniku) ali odobren vsiljivcu. V prvem primeru gre za napako tipa I, ki jo izrazimo kot stopnjo napačne zavrnitve – FRR (angl. False Rejection Rate). V drugem primeru gre za napako tipa II, ki jo izrazimo kot stopnjo napačnega sprejema – FAR (angl. False Acceptance Rate).

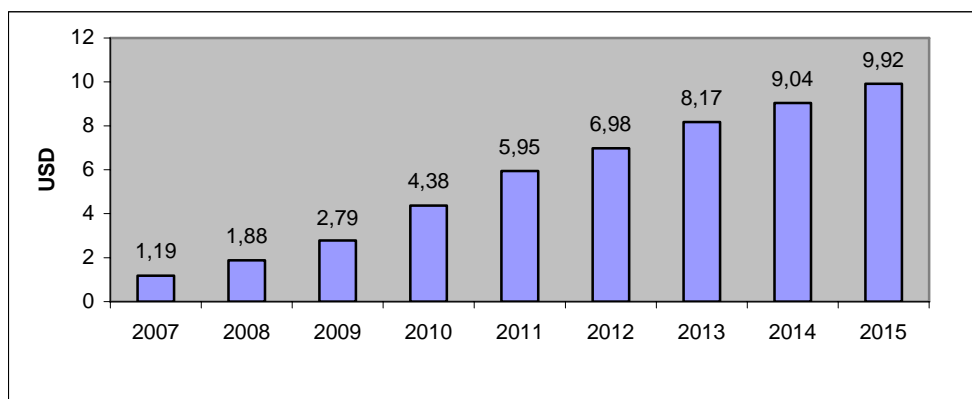
Vrednosti FAR in FRR sta povezani. Stopnjo FAR lahko zmanjšamo tako, da povečamo občutljivost sistema, vendar se s tem poveča FRR. Z zmanjšano občutljivostjo sistema zmanjšamo FRR, vendar s tem zmanjšamo varnost, saj se poveča FAR. Ker se lastnosti izključujeta, moramo najti kompromis. Izberemo tako občutljivost sistema, da sta FAR in FRR čim manjši. Kjer se FAR in FRR izenačita, dobimo stopnjo enake napake – EER (angl. Equal Error Rate). Manjša ko je vrednost EER, bolj točen je sistem.

Omenjeno pa vpliva tudi na stroške. Nižjo EER bomo dosegli z občutljivejšimi sistemi, ki so obenem tudi dražji od manj občutljivih.

1.4 Trendi v biometriji

Biometrična industrija je v preteklih letih beležila precejšnjo rast, ki se bo nadaljevala tudi v prihodnjih letih. V letu 2007 je prihodek panoge znašal nekaj manj kot 1,2 milijardi USD, napoved za leto 2015 pa znaša skoraj 10 milijard USD. Do takšne rasti bo prišlo zaradi tehnoloških zmožnosti, ki bodo poenostavile uporabo ter povečale točnost in zmogljivost biometričnih sistemov.

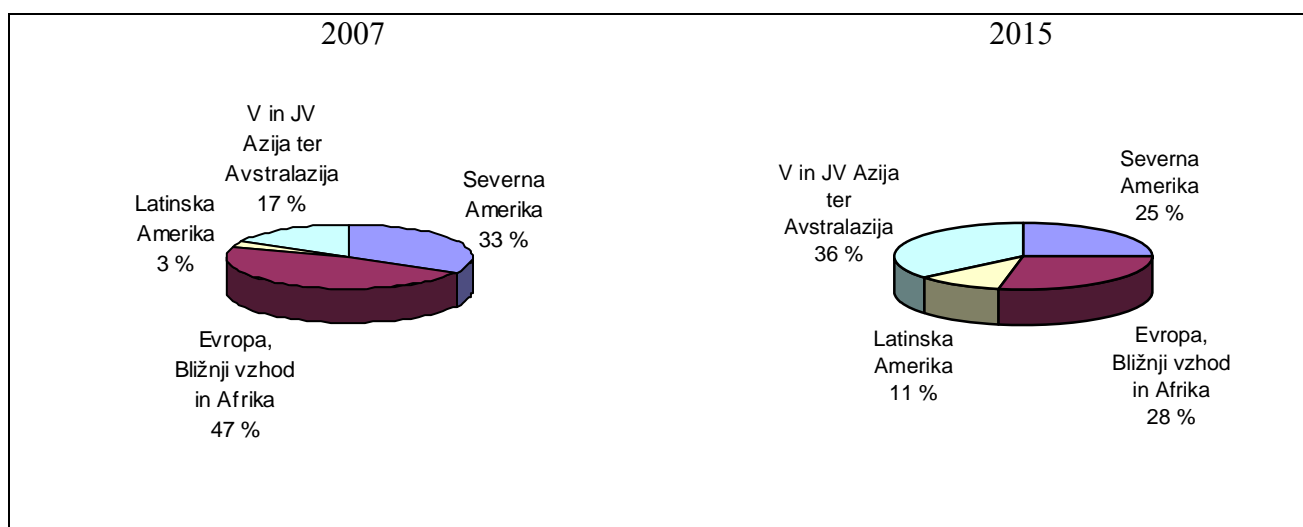
Slika 3: Letni prihodki v biometrični industriji v obdobju 2007–2015 (v milijardah USD)



Vir: *The Future of Biometrics*, 2009

Slika 4 ponazarja tržne deleže biometrične industrije po regijah za leti 2007 in 2015. Če deleže primerjamo, sta najbolj opazna padec tržnega deleža, ki ga imajo Evropa, Bližnji vzhod in Afrika, ter povečanje tržnega deleža v in JV Azije ter Avstralazije.

Slika 4: Tržni deleži po regijah v letih 2007 in 2015



Vir: *The Future of Biometrics*, 2009

1.5 Standardi in zakonodaja

S standardizacijo biometričnih sistemov se ukvarjata organizaciji ISO¹ (standard ISO/IEC JTC1 SC 37) in DIN² (standard DIN NI-37).

Biometrične značilnosti štejemo kot osebne podatke in jih kot take ureja Zakon o varstvu osebnih podatkov (ZVOP-1)³, členi 78–81.

2 Informacijski sistemi

2.1 Splošno o informacijskih sistemih

Informacijski sistem je sistem, v katerem se generirajo, arhivirajo in pretakajo sporočila in informacije (Gradišar & Resinovič, 1996, str. 92).

Informacijski sistem v podjetju je sistem, v katerem se ustvarjajo, shranjujejo in pretakajo informacije, ki so osnova za vsako aktivnost v podjetju (Gradišar et al., 2005, str. 39).

Informacijski sistem lahko definiramo kot množico ljudi, strojev, idej, aktivnosti, podatkov in postopkov, ki skupaj omogočajo pridobitev koristnih informacij (Damij & Štemberger, 1995, str. 6).

Tako vidimo, da je cilj informacijskih sistemov (v nadaljevanju IS) posredovanje informacij med pošiljateljem in prejemnikom, pri čemer je treba premostiti lokacijsko in časovno oviro. Iz tega lahko ugotovimo temeljne funkcije IS. Prva funkcija IS je zbiranje podatkov. Zbira se jih z namenom posredovanja uporabnikom, ki jih potrebujejo. Ker uporabnik podatkov oz. informacij ne uporabi takoj, ko so zajete, oz. ker so podatki in informacije lahko uporabni večkrat, jih je potrebno tudi shraniti. Podatki v IS so lahko uporabniku neuporabni, če mu niso podani v pravi obliki, zato je pomembna še četrta temeljna funkcija IS – obdelovanje podatkov.

2.2 Schengenski informacijski sistem

2.2.1 Schengen

Izraza »Schengen« oz. Schengenski sporazum uporabljamo za mednarodna sporazuma, ki sta bila podpisana v kraju Schengen v Luksemburgu (Schengenski sporazum in Schengenska

¹ Mednarodna organizacija za standardizacijo (angl. International Organization for Standardization)

² Nemški inštitut za standardizacijo (nem. Deutsches Institut für Normung)

³ Uradni list RS, št. 94/2007 z dne 16. 10. 2007

konvencija). Ime kraja je postalo sinonim za odpravo mejnega nadzora na notranjih mejah schengenskih držav članic.

Schengenski sporazum (Uradni list L 239, 2000a), znan tudi kot Schengen I, je bil podpisan 14. junija 1985. Države podpisnice so bile države Beneluksa, Zvezna republika Nemčija in Francija. Šlo je za sporazum o postopni ukinitvi nadzora na skupnih notranjih mejah.

Drugi sporazum, znan tudi kot Schengen II, Schengenska konvencija (Uradni list L 239, 2000b), je bil podpisan 19. junija 1990. To je bil sporazum o izvajanju Schengenskega sporazuma iz leta 1985. Konvencija je začela veljati 1. septembra 1993, vendar so jo prve države začele uporabljati v praksi šele marca 1995.

Med schengenske ukrepe uvrščamo vzpostavitev skupnih pravil za kontrole na zunanjih mejah, določanje skupne vizumske politike in uvajanje spremljevalnih ukrepov, ki omogočajo odpravo kontrol na notranjih mejah (zlasti na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah).

Ta pravila torej na državljane vplivajo neposredno, saj predvidevajo:

- odpravo mejnega nadzora na skupnih notranjih mejah,
- skupno zbirko pravil za osebe, ki prehajajo zunanje meje držav članic schengenskega območja,
- ločevanje oseb, ki potujejo znotraj schengenskega območja, od tistih, ki prihajajo iz držav izven schengenskega območja, na letaliških terminalih in, kadar je mogoče, v pristaniščih,
- uskladitev pravil v zvezi s pogoji vstopa in vizumi za kratkoročno prebivanje.

Temeljna ideja Schengena je torej zagotovitev prostega prehajanja notranjih meja. Zaradi ukinitve meja bi utegnilo priti do zmanjšanja varnosti v schengenskih članicah, zato so nujni izravnalni ukrepi ki se jih izvaja na zunanjih mejah območja, v notranjosti držav (skozi čezmejno policijsko sodelovanje), v okviru skupnega informacijskega sistema, imenovanega Schengenski informacijski sistem (SIS), ter skozi harmonizacijo zakonodaje v državah članicah.

V tabeli 2 je podan časovni pregled integracije od njenega začetka leta 1985 pa do 29. marca 2008, ko so bile v Sloveniji odpravljene kontrole tudi na zračnih mejah.

Tabela 2: Časovni pregled integracije

1985	Schengenski sporazum: Belgija, Nizozemska, Luksemburg, Nemčija in Francija podpišejo sporazum o postopni odpravi kontrol na skupnih mejah. Sporazum je podpisan v luksemburški vasi Schengen.
1990	Podpis Schengenske konvencije o izvajanju Schengenskega sporazuma iz leta 1985.
1990–1992	Schengensko konvencijo podpišejo Italija, Španija, Portugalska in Grčija.
1995	Schengenska konvencija začne veljati in odpravlja kontrole na notranjih mejah držav podpisnic (Beneluks, Francija, Nemčija, Španija in Portugalska) ter vzpostavlja enotno zunanjo mejo, kjer se skladno z enotnimi pravili izvaja kontrola vstopa v schengensko območje. Določijo se "izravnalni" ukrepi (skupna vizumska politika, boljše sodelovanje na področju policije in pravosodja ter schengenski informacijski sistem). Schengensko konvencijo podpiše Avstrija.
1996	Schengensko konvencijo podpišejo Danska, Finska in Švedska. Konvencijo na podlagi prejšnjih sporazumov med nordijskimi državami o odpravi mejne kontrole podpišeta tudi Islandija in Norveška, čeprav nista članici Evropske unije.
1999	Začne veljati Amsterdamska pogodba. Schengenski pravni red se v Evropsko unijo prenese s Protokolom k Amsterdamski pogodbi. Protokol določa tudi, da sta Združeno kraljestvo in Irska lahko udeležena v vseh ali nekaterih schengenskih ureditvah, če to soglasno odobri Svet.
2000	Odpravljene so kontrole na notranjih mejah z Grčijo. Ugodi se prošnji Združenega kraljestva za delno sodelovanje v "schengenu" (v glavnem na področju policijskega sodelovanja in sodelovanja na področju pravosodja ter delnega sodelovanja v SIS).
2002	Ugodi se prošnji Irske za delno sodelovanje v "schengenu" (prav tako v glavnem na področju policijskega sodelovanja in sodelovanja na področju pravosodja ter delnega sodelovanja v SIS).
Maj 2004	Pristop novih držav članic: Ciper, Slovaška, Slovenija, Estonija, Madžarska, Latvija, Litva, Malta, Poljska in Češka. Svet Evrope in Haaški program kot rok njihove vključitve v schengensko območje določita oktober 2007.

»se nadaljuje«

»nadaljevanje«

2004	Švica podpiše sporazum o pridružitvi "schengenu". Združeno Kraljestvo začne izvajati nekatere schengenske določbe (čeprav še ni priključeno na SIS).
2006	Lihtenštajn izda protokol o priključitvi k švicarskemu sporazumu o pridružitvi.
Sept. 2006	Evropska komisija napove, da po vsej verjetnosti SISII ne bo začel delovati do oktobra 2007. Portugalska napove, da bo razvila prehodno tehnično rešitev SISone4ALL (SIS I za vse).
16. okt. 2006	Svet za pravosodje in notranje zadeve da zeleno luč za predhodna tehnična dela za testiranje SISone4ALL.
5. dec. 2006	Svet za pravosodje in notranje zadeve dokončno odobri SISone4ALL in 31. december 2007 postavi kot rok za odpravo meja.
2007	Bolgarija in Romunija vstopita v Evropsko unijo in delno izvajata schengenske določbe. Kontrole na notranjih mejah se odpravijo, ko so vzpostavljeni vsi izravnalni ukrepi in ko Svet sprejme pozitivno evalvacijsko poročilo.
2. marec 2007	SISone4ALL je uspešno testiran na C-SIS.
27. marec 2007	Podpis protokola med Portugalsko in devetimi državami članicami, ki bodo uporabljale sistem SISone4ALL.
1. maj 2007	PT NSIS je uspešno testiran na C-SIS.
26. junij 2007	SISone4ALL potrdijo nove države članice.
14. avg. 2007	SISone4ALL potrdijo države članice schengenskega območja.
31. avg. 2007	SISone4ALL je tehnično pripravljen.
Sept./Dec. 2007	Zadnja faza evalvacije novih držav članic. SISone4ALL je ocenjen pozitivno.
6. dec. 2007	Odločitev Sveta o odpravi mejnih kontrol na vseh notranjih mejah.
21. dec. 2007	Odprava mejne kontrole na kopenskih in morskimi mejah.
29. marec 2008	Odprava mejne kontrole na zračnih mejah.

Vir: Širitev Schengenskega območja, 2008

2.2.2 Schengenski pravni red

Schengenski pravni red je bil leta 1999 z Amsterdamsko pogodbo vključen v okvir pravnega reda EU. Predstavlja zbirko pravil, ki so bila sprejeta v okviru medvladne schengenske skupine in vključujejo:

- Schengenski sporazum iz leta 1985,
- Konvencijo o izvajanju Schengenskega sporazuma iz leta 1990,

- pristopne protokole, sklenjene z Italijo, Španijo, Portugalsko, Grčijo, Avstrijo, Dansko, Finsko in Švedsko,
- sporazum z Norveško in Islandijo,
- posebna sporazuma z Veliko Britanijo in Irsko ter
- sklepe in izjave, ki so jih sprejeli schengenski organi.

V Schengenski pravni red so vključeni številni ukrepi, med njimi tudi ukrepi, namenjeni povečanju varnosti na zunanjih mejah EU, saj se zaradi ukinitve notranjih meja tam kontrole ne izvajajo več.

Najpomembnejši med temi ukrepi zahteva, da države članice na svojih zunanjih mejah EU zagotavljajo izvajanje ustreznih kontrol in učinkovit mejni nadzor. Zaradi prostega gibanja znotraj schengenskega območja je to izrednega pomena. Na zunanjih mejah morata biti preverjanje in kontrola dovolj stroga, da ustavita nezakonito priseljevanje, tihotapljenje drog in druge nezakonite dejavnosti.

V primeru grožnje javnemu redu ali javni varnosti lahko na podlagi zaščitne klavzule katera koli država članica ponovno vzpostavi kontrole na svojih mejah znotraj Evropske skupnosti. Eden takih primerov se je zgodil junija 2008, ko je Avstrija gostila evropsko prvenstvo v nogometu.

2.2.3 Schengenski informacijski sistem

Schengenski informacijski sistem (SIS) je pomemben del schengenskega pravnega reda. Gre za obsežno bazo podatkov, ki deluje kot skupni informacijski sistem, ki uporabnikom (policija, carina, upravne enote in konzularni uslužbenci iz držav podpisnic ...) omogoča izmenjavo podatkov, kot so npr. podatki o osumljencih kaznivih dejanj, pogrešanih osebah, državljanih tretjih držav, ki jim je zavrjen vstop ipd., ki jih potrebujejo za vzpostavitev območja brez kontrol na notranjih mejah.

Vsi podatki SIS so shranjeni v centralnem sistemu (C-SIS) v Strasbourgu v Franciji. Poleg centralnega sistema je SIS sestavljen tudi iz nacionalnih sistemov (N-SIS), ki se nahajajo v državah članicah. Države podatke v SIS vnašajo prek nacionalnih sistemov, prav tako pa prek njih izvajajo poizvedovanje v skupni bazi podatkov.

Vse države članice morajo v podporo delovanju sistema ustanoviti urad SIRENE⁴, ki deluje kot operativno-komunikacijski center policije za področje SIS. Glavne naloge urada se nanašajo predvsem na izmenjavo dodatnih informacij:

- pred razpisom tiralice,
- istočasno oz. vzporedno z razpisom tiralice,

⁴ Supplementary Information Request at the National Entry

- v primeru večkratnega razpisa tiralice,
- v primeru označitve tiralice (flag),
- v primeru zadetka (hit),
- v primeru razpisa ukrepa zavrnitve vstopa državljanov iz tretjih držav,
- nezmožnosti izvajanja določenega ukrepa, ki je predviden v primeru zadetka,
- v primeru spremembe namena in
- v primeru nepravilnosti podatkov ali v primeru nezakonito shranjenih podatkov in o pravici vpogleda v lastne podatke in pravici do poprave podatkov.

Uradi SIRENE pri vseh kategorijah razpisov opravijo naloge, ki se nanašajo na:

- preveritev skladnosti postopka z določbami Schengenskega izvedbenega sporazuma,
- preveritev tehnične kvalitete podatkov,
- upoštevanje predpisanega vrstnega reda postopkov,
- takojšnje obveščanje razpisnika v primeru zadetka in
- izmenjavo dodatnih informacij.

Poleg glavnih nalog imajo ti uradi tudi dodatne naloge, ki se nanašajo na kontinuirano, pospešeno mednarodno policijsko sodelovanje:

- izmenjava informacij na področju policijskega sodelovanja,
- razpisovanje tiralic in izmenjava informacij v okviru SIS ima prednost pred razpisovanjem in izmenjavo informacij preko Interpola (razpisa zoper isto osebo se ne izključujeta).

Nekatere naloge, ki jih opravljajo uradi SIRENE, se prekrivajo s tistimi, ki jih opravlja Interpol, vendar njihov namen ni nadomestitev ali posnemanje Interpola.

Razpisi v SIS in ustrezne spremembe podatkov imajo vedno prednost pred razpisi in izmenjavami informacij preko Interpola. Ta prednost še posebej velja v primeru nasprotij med razpisom iz SIS in iz Interpola. V okviru schengena je prednost dana razpisom SIS pred razpisi Interpola.

Zelo pomemben del schengenskega sistema je tudi skupna vizumska politika in praksa, ki obsega:

- skupen vizumski režim (enotno listo tretjih držav, katerih državljani potrebujejo vizume),
- izdajanje enotnih vizumov, ki omogočajo gibanje po celotnem schengenskem ozemlju in
- usklajen postopek izdaje vizumov.

Države so uskladile tudi pogoje za vstop državljanov tretjih držav in njihovo bivanje na območju schengena (glede maksimalne dolžine bivanja na celotnem ozemlju držav članic,

pravice do tranzita, obveznosti policijske prijave, obveznosti odstranitve tujcev, če ne izpolnjujejo pogojev za bivanje, kazni za nedovoljen prehod meje, še posebej za prevoznike).

Kot že omenjeno, SIS v vsaki državi pogodbenici obsega nacionalne podatkovne zbirke in tehnični podporni del v Strasbourgu. Ta z on-line prenosom informacij zagotavlja, da nacionalni sistemi vsebujejo enake podatke. Sistem kot celota omogoča tako povezavo med nacionalnim in centralnim sistemom kot tudi povezavo med nacionalnimi sistemi držav pogodbenic.

2.2.3.1 Podatki v SIS

Schengenska baza podatkov v osnovi vsebuje dve vrsti podatkov:

- podatke o iskanih ali pogrešanih osebah in osebah pod tajnim sledenjem ter
- podatke o ukradenih ali drugače odtujenih vozilih in predmetih, kot so predvsem osebni dokumenti.

Zaradi narave podatkov o osebah se zanje uporablja določila Schengenske konvencije, določila Zakona o varstvu osebnih podatkov ter določila Konvencije Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov.

Schengenska konvencija omejuje nabor osebnih podatkov na podatke o:

- osebah, za katere se zaprosi za prijetje zaradi izročitve (95. člen Schengenske konvencije),
- osebah, ki niso državljani držav članic, za katere je razpisana zavrnitev vstopa v schengensko območje (96. člen Schengenske konvencije),
- pogrešanih osebah ali osebah, ki potrebujejo začasno policijsko zaščito, predvsem mladoletnih (97. člen Schengenske konvencije),
- pričah oziroma osebah, ki se morajo v okviru kazenskega postopka zglasiti na sodišču ali jim je potrebno vročiti sodbo ali vabilo na prestajanje kazni (98. člen Schengenske konvencije) in
- osebah za namene tajnega opazovanja ali namenske kontrole (99. člen Schengenske konvencije).

Pri tem so lahko za osebe zabeleženi samo naslednji podatki:

- priimek in ime, morebiten alias, po potrebi v novem podatkovnem zapisu,
- morebitne objektivne fizične posebnosti, ki se ne spreminjajo,
- prva črka drugega imena,
- datum in kraj rojstva,
- spol,
- državljanstvo,
- ali so bile te osebe oborožene,

- ali so bile te osebe nasilne,
- razlog za razpis ukrepa,
- predlagana oblika ukrepanja.

Poleg navedenih osebnih podatkov SIS vsebuje tudi podatke o:

- vozilih, za katere se izvaja tajno opazovanje ali namenska kontrola (99. člen Schengenske konvencije) in
- predmetih, ki se iščejo zaradi zasega ali za zagotovitev dokazov v kazenskih postopkih (100. člen Schengenske konvencije).

Nikakršni drugi osebni podatki, zlasti občutljivi, kot so npr. o rasnem poreklu, političnih, verskih ali drugih prepričanjih itd., niso dovoljeni. Vsi podatki, ki se nahajajo v sistemu, lahko osebe, ki jim je dostop dovoljen, uporabljajo le v skladu z nameni, ki so opredeljenimi s Schengensko konvencijo.

Organi, ki so pristojni za dostop do podatkov v SIS in njihovo uporabo so:

- policija pri opravljanju mejne kontrole in drugih policijskih preverjanj v notranjosti države,
- diplomatsko-konzularna predstavništva v Sloveniji in tujini ob izdaji vizuma,
- ministrstvo za notranje zadeve pri obravnavi prošenj za izdajo vizumov,
- upravne enote v postopkih s tujci ter pri registraciji motornih vozil in izdaji registrskih tablic,
- pristojni pravosodni organi v državah članicah ter
- EUROPOL in EUROJUST.

V podatke v zvezi z zavrnitvijo vstopa tujcu po 96. členu in v zvezi z osebnimi dokumenti iz člena 100 (točki d in e 3. odstavek) Schengenske konvencije, ki so bili ukradeni, protipravno odvzeti ali drugače odtujeni (potni listi, osebne izkaznice, vozniška dovoljenja), imajo vpogled še:

- službe, pristojne za dodeljevanje vizumov,
- centralni organi, pristojni za obdelavo prošenj za vizum,
- službe, pristojne za dodeljevanje dokumentov o bivanju in
- službe, pristojne za izvajanje Zakona o tujcih.

Nadalje imajo pravico dostopa do podatkov o ukradenih, protipravno odtujenih ali izgubljenih vozilih (točki a in b 100. člena Schengenske konvencije) ter podatkov o ukradenih, protipravno odtujenih, izgubljenih ali preklicanih prometnih dovoljenjih in registrskih tablicah vozil tudi vladne in druge službe, ki so v državah članicah EU odgovorne za izdajanje potrdil o registraciji vozil iz Direktive Sveta 1999/37/ES z dne 29. aprila 1999 o dokumentih za registracijo vozil.

V okviru navedenega mora država pogodbenica določiti seznam organov, ki so pooblašteni za dostop do podatkov v SIS, in ga posredovati Izvršnemu odboru, ki je bil ustanovljen za namene izvajanja Schengenske konvencije.

V Schengenski konvenciji, Zakonu o varstvu osebnih podatkov in Zakonu o informacijskem pooblaščenju je navedeno, da ima vsak posameznik pravico do seznanitve z osebnimi podatki v SIS, ki so zabeleženi o njem, ter do popravka in izbrisa napačnih podatkov.

Tako ima vsakdo na ozemlju katere koli države v schengenskem območju pravico, da na sodišču ali pri drugem po nacionalni zakonodaji pristojnem organu, zahteva popravek, izbris, pridobitev informacije ali odškodnino v zvezi z razpisom ukrepa, ki se nanaša nanj. Glede na to, da so podatki v vseh nacionalnih sistemih identični, se lahko pravica do vpogleda, popravka ali izbrisa nanaša na podatke ne glede na državo, pri kateri je vložena zahteva. Ker pa postopek teče po nacionalnem pravu tiste države, kjer je bila zahteva vložena, se ta v podrobnostih razlikuje med posameznimi državami.

2.2.4 SIS I+

Leta 1998 je bila opravljena predhodna študija za oceno morebitnega razvoja in izboljšav SIS. Tako je bila, tudi zaradi hitrejše priključitve petih nordijskih držav, razvita posodobljena različica sistema, imenovana SIS I+. Ta je tudi po priključitvi novih članic še vedno omogočala priključitev še dveh ali treh držav. S posodobitvijo so izboljšali zmogljivosti sistema ter olajšali njegovo upravljanje in vzdrževanje. Prenovljeni sistem je vseboval tudi določene spremembe zaradi premostitve težav z letom 2000.

2.2.5 SIS II

Zaradi omejitev obstoječega sistema na največ 18 držav je bilo nujno potrebno razviti nov sistem, ki bo državam članicam omogočil celovito izvajanje schengenskega pravnega reda in odpravo kontrol na njihovih notranjih mejah z drugimi državami v schengenskem območju.

Poleg povečanja zmogljivosti glede števila sodelujočih držav je namen SIS II tudi izboljšanje varnosti in učinkovitejša uporaba podatkov. Z novim sistemom bi se vpeljale tudi dodatne funkcionalnosti, ki jih omogoča najnovejši tehnološki razvoj. Odlika sistema bi bila tudi dobra prilagodljivost in bi se kot tak lahko kosal s spreminjajočimi se zahtevami.

06. 12. 2001 je Svet pooblastil Komisijo, da razvije SIS II, ki bi se financiral iz proračuna EU. Tehnično izvedbo je Komisija začela oktobra 2004, ko je bila podpisana pogodba o razvoju SIS II, skupaj s SIS II pa bi razvili tudi VIS (vizumski informacijski sistem), saj si sistema delita isto tehnično osnovo. SIS II naj bi bil dokončan v marcu 2007, konec leta 2007 pa naj bi se nanj priključile nove države članice EU, ki so se pridružile maja 2004.

Skupaj s tehnično izvedbo so potekale tudi razprave o novih zahtevah sistema. SIS II je potreboval primeren pravni okvir, kjer bi bilo podrobno opisano delovanje in uporaba sistema. 01.06.2005 je Komisija zaradi različnih političnih področij, vložila tri zakonodajne predloge.

Prvi predlog je temeljil na naslovu IV Pogodbe o ES (vizumi, azil, priseljevanje in druge politike v zvezi s prostim gibanjem oseb), drugi pa na naslovu VI Pogodbe o EU (policijsko in pravosodno sodelovanje v kazenskih zadevah). Ta dva predloga je dopolnjeval tretji predlog, ki je temeljil na naslovu V Promet. Njegov namen je bil zagotavljanje dostopa do SIS II organom, ki so pristojni za izdajanje potrdil o registraciji vozil. Kljub obstoju treh zakonodajnih besedil, ki so uvrščena v postopek soodločanja in postopek posvetovanja, gre za enoten paket, saj SIS II deluje kot en sam informacijski sistem.

Omenjeni predlogi so bili Evropskemu parlamentu poslani z zamudo, poleg tega pa je manjkala tudi zelo pomembna obrazložitev predlogov, ki so bili tehnično zelo zahtevni in zapleteni.

Zaradi zapletenosti pogajanj je bil kompromis glede končnega besedila med Evropskim parlamentom, Komisijo in Svetom, dosežen 27. 09. 2006. Ta kompromisni paket je bil 5. oktobra skoraj soglasno sprejet v Odboru za državljanske svoboščine, pravosodje in notranje zadeve. Z veliko večino pri glasovanju je bil potrjen tudi na plenarnem zasedanju 25. oktobra 2006.

Kljub uspešnosti Evropskega parlamenta pri pospešitvi postopka za sprejetje pravnih instrumentov o SIS II so nastale zamude pri projektu. Junija 2006 je bilo jasno, da bo treba popraviti časovni načrt, saj sistem do marca 2007 ne bo usposobljen, ker je bil manevrski prostor za zamude že porabljen. Razlogov za to je bilo več:

- izvajalci, ki v razpisnih postopkih za oblikovanje novega sistema niso bili izbrani, so glede tega sprožili postopke pred sodiščem,
- Komisija je imela težave tudi z izvajalci, ki jih je najela za oblikovanje te baze podatkov, njen zagon in upravljanje z njo,
- zamude pri pripravljalnih delih, povezanih z osrednjim objektom v Strasbourgu, kjer bo sedež baze podatkov. Komisija je priznala, da predlaganega sedeža v Strasbourgu ni mogoče pravočasno pripraviti, da bi lahko v skladu s časovnim načrtom tja dostavili opremo, potrebno za SIS II,
- tehnične težave tako v nekaterih državah članicah kot tudi pri razvoju centralnega SIS.

Pri revidiranju celotnega časovnega načrta projekta bi bilo treba poskušati čim bolj zmanjšati obseg posledic te zamude v državah članicah, ki izpolnjujejo zahtevane pogoje za vstop v schengensko območje.

Po mnenju nekaterih držav članic, ki čakajo na vstop v schengen, naj bi poleg omenjenih razlogov, za zamudo obstajali tudi politični razlogi. Obstoječe članice schengena naj ne bi zaupale v zmožnost novih članic pri izpolnjevanju obveznosti, ki jih članstvo v schengenu prinaša. Zato naj bi si želele, da se schengensko območje poveča, šele ko bo vzpostavljen SIS II.

Johnatan Faull, direktor generalnega direktorata Evropske komisije za pravosodje, svobodo in varnost, je zanikal, da bi bili v ozadju politični razlogi. Franco Frattini, evropski komisar za pravosodje, svoboščine in enake možnosti, pa je dodal, da je med novinkami samo Slovenija pripravljena na vstop v območje schengena.

2.2.5.1 SISone4all (SIS I za vse)

Oktobra 2006 je bila potrjena nova časovnica, ki je predvidevala, da naj bi bil SIS II operativen šele junija 2008, vstop novih članic pa naj bi se zgodil šele v letu 2009.

Nove članice so se na zamudo odzvale ogorčeno, saj so v izpolnjevanje postavljenih kriterijev vložile veliko naporov in sredstev.

Kot rešitev je Portugalska predlagala modificirano verzijo svojega SIS I+ sistema, katerega bi nove članice uporabljale do uvedbe SIS II. Tako bi lahko nove članice, ki bodo pripravljene, v schengen vstopile že konec leta 2007.

Sistem je sestavljen iz centralnega (C.SIS) in nacionalnega dela (N.SIS). Izmenjava informacij med C.SIS in N.SIS je natančno predpisana, medtem ko je implementacija N.SIS je prepuščena posameznim članicam. Vključitev po sistemu SISone4all pomeni, da novinke prevzamejo portugalsko implementacijo N.SIS. S tehnične plati to pomeni, da Portugalska dobavi programsko opremo, novinke pa strojno opremo, komunikacijsko infrastrukturo in ostale dejavnosti.

Način vključitve SISone4ALL, ki predstavlja portugalsko implementacijo N.SIS, je pomenil za Slovenijo in ostale nove države članice vključitev v SIS, ob uspešno opravljeni evalvaciji ter globalnem testiranju pa bi prišlo tudi do povečanja schengenskega območja.

Taka vključitev bi prihranila precej časa, saj je portugalska implementacija N.SIS že stestirana, s čimer bi bil obseg testiranja v novih članicah precej zmanjšan. V primeru večjih težav pri testiranju ali evalvaciji bi se širitev območja na novo državo odložila, v primeru manjših težav pa se rok vključitve ne bi spreminjal, država članica pa naj bi težave čim hitreje odpravila.

Kopenske in zračne meje naj bi bile tako odpravljene najpozneje do 31. 12. 2007, zračne pa marca 2008. Slednje se lahko odpravijo le ob prehodu s poletnega na zimski vozni red oz. ob prehodu z zimskega na poletni vozni red.

Slovenija naj bi za vključitev v schengenski sistem porabila približno milijon evrov, za razširitev SIS I+ pa še približno 100.000 evrov.

Nove članice so postale del schengenskega območja 21. decembra 2007, razvoj SIS II pa se je nadaljeval. Ko je bilo jasno, da SIS II ne bo pripravljen do junija 2008, je bila postavljena nova časovnica – sistem naj bi bil operativen šele septembra 2009.

Decembra 2008 je bilo izvedeno testiranje sistema, kjer sta bili ugotovljeni dve večji pomanjkljivosti:

- Nezmožnost komunikacije računalnikov v državah članicah s centralizirano podatkovno bazo v Strasbourgu,
- nekateri podatki, ki so bili poslani v sistem, so se izgubili.

Zaradi teh napak vzpostavitve sistema v septembru 2009 ni več realistična. 15. in 16. januarja 2009 je v Pragi potekalo neformalno zasedanje notranjih ministrov EU. Odločili so se, da bo novi sistem podvržen temeljiti tehnični, pravni in finančni analizi z načrtom za odpravo napak. Analiza naj bi bila dokončana najpozneje do junija – takrat naj bi bila znana tudi usoda SIS II. Ena možnost je izpeljava projekta do konca, drugo pa predstavlja alternativni scenarij, ki predvideva nadgradnjo sedanjega sistema na podlagi sistema SISone4ALL, kateremu se je poleg Slovenije in še osmih držav v decembru 2007 decembra 2008 pridružila tudi Švica.

V primeru nadaljevanja projekta bi bil SIS II v najboljšem primeru vzpostavljen šele leta 2010, pri vstopu v schengenski prostor pa bi utegnil ogroziti Bolgarijo in Romunijo, ki naj bi se priključili leta 2011.

2.2.5.2 Migracija s SIS I+ na SIS II

Prvotni načrt migracije je vključeval le 15 držav članic (tedanje število), končana pa naj bi bila v približno osmih urah.

Sedanji sistem ima 10 članic več, s čimer je migracija na novo omrežje precej bolj zapletena. Zaradi tega bi se lahko zgodilo, da katera izmed držav ne bi mogla uspešno izvesti migracije. Če bi prišlo do tega, bi bila posledica ponovna vzpostavitve meja te države.

Prav zaradi tega je bilo treba poiskati nadomestno rešitev, ki bi v primeru težav omogočila vrnitev na sistem SIS I+.

Tako bo v tem kratkem obdobju prehoda omogočeno vzporedno delovanje nekaterih delov tehničnih arhitektur obeh sistemov. Po prehodu bo na voljo tehnično orodje, ki bo omogočalo uspešno pretvarjanje in usklajevanje podatkov med obema sistemoma. Ta pretvornik bo povezoval centralna sistema obeh sistemov, s čimer bosta oba obdelovala iste podatke. Na ta način ostanejo tako države, ki so že izvedle prehod, kot tudi tiste, ki ga še niso, na enaki ravni.

Cilj predloga Komisije ni le oblikovati pravni okvir za migracijo, ampak tudi celovit preskus, zlasti da bi se pokazalo, da je raven uspešnosti delovanja SIS II najmanj enakovredna ravni SIS I+. Poleg tega bo predlog urejal izvedbo preskusa izmenjave dopolnilnih podatkov.

Pred migracijo na novi sistem bi bilo treba izpolniti pogoje, navedene v členu 55(3) uredbe 1987/2006:

- sprejetje potrebnih izvedbenih ukrepov,
- poročanje držav članic o sprejetju potrebnih tehničnih in pravnih ureditev za obdelavo in izmenjavo podatkov,
- uspešno opravljen celovit preskus,
- sprejetje potrebnih tehničnih ureditev za povezavo centralnega SIS II z nacionalnim sistemom.

Z operativnim zagonom sistema se konča faza razvoja; začne se izvrševanje pravne podlage SIS II.

2.2.6 Uvajanje schengenskega sistema v Sloveniji

Ko je Slovenija 1. maja 2004 postala članica EU, je v skladu s pristopno pogodbo prevzela dolžnost izvajanja schengenskega pravnega reda v celoti. Na mejah z državami članicami je bil ohranjen samo še poenostavljen policijski nadzor, carinskega pa ni bilo več. Na meji s Hrvaško je bil vzpostavljen varnostni, carinski in inšpekcijski nadzor, delno pa so se izvajala tudi določila schengenskega pravnega reda.

Veliko dela s pripravami na vstop v schengen je imela predvsem policija.

- Usklajevanje s pravnim redom EU

Policija je aktivno sodelovala pri medresorskih usklajevanjih, dogovarjanjih in implementaciji bilateralnih in drugih sporazumov.

- Organizacijsko-kadrovske priprave

V skladu s schengenskim izvedbenim načrtom je bilo za status policista odprtih 3092 delovnih mest. Zaposlovanje za potrebe varovanja državnih meja se je začelo že leta 2001.

Ko so bile odpravljene mejne kontrole na notranjih mejah, je prišlo do prerazporeditev kadrov z notranje na zunanjo mejo in v policijske postaje za izravnalne ukrepe. Na zunanjo mejo je bilo premeščenih 460 policistov, ki so v večini primerov prišli iz policijskih uprav Slovenj Gradca, Nove Gorice in Kopra.

- Izpopolnjevanje in usposabljanje

Za varovanje zunanje schengenske meje je v policiji potekalo dodatno usposabljanje. V obdobju od leta 1999 do junija 2007 so v okviru twinning projektov (partnersko sodelovanje) potekala usposabljanja policistov inštruktorjev, ki so jih izvajali strokovnjaki iz Avstrije,

Nemčije, Italije in Španije. Policisti inštruktorji so pozneje ta znanja prenesli policistom na regionalno in lokalno raven.

- Nabava tehnične opreme

Sem spada oprema, ki je potrebna za opravljanje nadzora državne meje po schengenskih kriterijih (službena vozila, helikopter, videonadzorni sistemi, snemalne naprave za mejne prehode, naprave za nočno opazovanje ...).

- Prilagajanje infrastrukture

Med Slovenijo in Hrvaško imamo 60 mejnih prehodov (skupaj s prehodi za obmejni promet). Z vstopom Slovenije v schengensko območje ni bil ukinjen noben mejni prehod. Investicije vanje naj bi bile zaključene najpozneje letos ali naslednje leto.

- Ukrepi na letališčih in pristaniščih

Zaradi izpolnjevanja schengenskih standardov je bilo potrebno odpraviti določene pomanjkljivosti na letališčih. Na letališču Jožeta Pučnika Ljubljana so tako izvedli ukrepe, s katerimi so omogočili ločitev potnikov schengenskih in neschengenskih letov. V Luki Koper so zgradili mejni prehod na RO-RO terminalu; nov potniški terminal, ki bo v skladu s schengenskimi standardi, pa je še v izgradnji.

- Ukrepi na notranjih mejah in v notranjosti države

Z ukinitvijo notranjih meja, se mejne kontrole izvajajo samo še na zunanjih mejah. Da ne bi prišlo do zmanjšanja varnosti v državah članicah, se izvajajo t. i. izravnalni ukrepi, s katerimi se izravna t. i. varnostni primanjkljaj. Ukrepi se izvajajo na notranjih mejah in v notranjosti države, skozi čezmejno policijsko sodelovanje v okviru SIS in skozi harmonizacijo zakonodaje držav članic.

Leta 2002 je bila ustanovljena Specializirana enota za nadzor državne meje (SENDM). V nekaterih policijskih upravah so bile ustanovljene policijske postaje za izravnalne ukrepe. Te enote se ukvarjajo s preprečevanjem čezmejne kriminalitete in ilegalnimi migracijami. Ker se nahajajo na območjih z notranjo državno mejo, je tu zaposleno tudi precej policistov, ki so bili pred tem zaposleni v enotah, ki so bile z vstopom v schengen ukinjene.

- Uresničevanje določil Schengenskega sporazuma na področju varstva podatkov

Glede varstva osebnih podatkov je za nadzor nacionalne podatkovne zbirke pristojen nacionalni nadzorni organ vsake pogodbenice. Pri nas je za to pristojen Informacijski pooblaščenec.

- Vzpostavitev urada SIRENE in drugih oblik mednarodnega policijskega sodelovanja

Urad SIRENE je bil ustanovljen v okviru Sektorja za mednarodno policijsko sodelovanje, in skrbi za komunikacijo s SIS in sistematično policijsko sodelovanje. Temelji tega sodelovanja so medsebojne izmenjave podatkov in razpisov za iskanje oseb in predmetov.

- Vzpostavitev SIS

Po integraciji nacionalnega sistema s centralnim sistemom in po uspešno opravljenih vseh testiranjih se je Slovenija že 1. septembra 2007 vključila v SIS I+.

- Financiranje uveljavitve schengenskih standardov nadzora državne meje

Zaradi visokih stroškov, ki nastanejo pri uvajanju schengenskih standardov, so novinke upravičene do finančne pomoči. Slovenija je dobila slabih 120 milijonov evrov, ki so namenjeni pokritju stroškov, ki so nastali od dneva pristopa v EU do konca leta 2006. Sredstva so v največji meri prišla iz Schengenskega vira (Schengen Facility), preostali del pa je prišel še iz sredstev rednega proračuna in sredstev predpristopne pomoči (PHARE, Transition Facility).

V nadaljevanju navajam časovnico pristopa Slovenije k schengenskememu sistemu:

1. maja 2004 je Slovenija postala članica EU. V skladu s pristopno pogodbo je prevzela dolžnost izvajanja schengenskega pravnega reda.

1. junija 2005 je Evropska komisija podala formalni predlog za vzpostavitev SIS II, ki je bil nujni pogoj za širitev schengenskega območja na deset novih članic EU. SIS II naj bi bil po načrtih pripravljen marca 2007.

V začetku junija 2005 je v Luksemburgu potekalo zasedanje notranjih ministrov EU, kjer so potrdili okvirno časovnico za širitev schengena na nove članice, sprejeli pa so tudi načrt evalvacijskih postopkov za vstop novih članic, ki je predviden za oktober 2007.

Decembra 2005 je Slovenija v Bruslju oddala vprašalnik za evalvacijo izpolnjevanja schengenskih standardov nadzora zunanje meje EU.

Februarja 2006 je v Sloveniji potekala schengenska evalvacija za področje policijskega sodelovanja. Marca, aprila in maja so sledile še evalvacija za področje varstva podatkov ter evalvaciji za področje morske in kopenske meje.

V začetku junija 2006 je avstrijska notranja ministrica Liese Prokop, takrat predsedujoča Svetu EU, priznala, da se širitev schengenskega območja zaradi težav pri vzpostavljanju SIS II lahko zavleče za nekaj mesecev, vendar so pozneje voditelji EU na vrhu v Bruslju vseeno potrdili časovnico za širitev schengenskega območja v oktobru 2007.

Konec junija 2006 je na brniškem letališču potekala schengenska evalvacija zračne meje. Infrastruktura ni bila v skladu s schengenskim pravnim redom, ker ni omogočala fizičnega ločevanja potnikov z območja schengena in tistih zunaj njega. 18. julija je sledil podpis pogodbe za obnovo in nadgradnjo obstoječega terminala na letališču Brnik.

24. julija 2006 je Franco Frattini, evropski komisar za pravosodje, priznal, da širitev schengenskega območja v oktobru 2007 ne bo mogoča saj SIS II ne bo pripravljen v zadanem roku.

22. septembra 2006 je bil s portugalske strani podan predlog SISone4all, ki naj bi omogočal, da bi se širitev v oktobru 2007 vseeno izvršila.

5. oktobra so notranji ministri EU sprejeli novo časovnico za širitev, po kateri naj bi bil SIS II operativen v juniju 2008.

13. oktober je v članicah EU v veljavo stopila Uredba o Zakoniku Skupnosti o pravilih, ki urejajo gibanje oseb preko meja (Zakonik o schengenskih mejah). Uredba določa standarde in postopke, po katerih se morajo ravnati članice pri izvajanju osebne kontrole na notranjih in zunanjih mejah EU.

Po preučitvi portugalskega predloga SIS I za vse je bil ta odobren na zasedanju v Bruslju 5. decembra 2006. Tako je bil cilj za odpravo nadzora na kopenskih in morskih mejah postavljen na december 2007, na letališčih pa na marec 2008.

27. marca 2007 so nove članice EU od Portugalske dobile simbolni paket programske opreme za projekt SIS I za vse.

12. april 2007 je vlada sprejela sklep o imenovanju medresorske delovne skupine za ureditev mejnih prehodov na notranjih mejah EU, ko bo mejna kontrola ukinjena.

26. maja 2007 je bilo sklenjeno testiranje sistema SIS I za vse. 7. junija je Evropski parlament podprl predlog Sveta EU o uporabi tega sistema in glasoval za razširitev schengenskega območja na devet novih članic EU, junija na zasedanju v Bruslju pa je Evropski svet potrdil časovnico, ki so jo določili decembra 2006.

V začetku julija 2007 je na letališču Brnik potekala ponovna evalvacija, ki ji je sledilo odprtje prve faze novega potniškega terminala ljubljanskega letališča, ki je dobilo novo uradno ime Letališče Jožeta Pučnika Ljubljana.

1. septembra 2007 je Slovenija začela uporabljati SIS I za vse, 2 tedna pozneje pa je sledila evalvacija uporabe sistema.

18. septembra 2007 so notranji ministri EU sprejeli odločitev, da bodo lahko hrvaški državljani v Slovenijo, Italijo in Madžarsko tudi po širitvi schengenskega prostora vstopali z osebnimi izkaznicami, vendar bodo morali imeti s seboj tudi posebne kartone z osebnimi podatki, ki se bodo žigosali ob vstopu in izstopu iz države.

6. novembra 2007 je bila širitev schengena napovedana za minuto čez polnoč v noči z 20. na 21. december.

8. novembra 2007 je Svet EU potrdil, da so vse schengenske kandidatke pripravljene na odpravo nadzora na svojih notranjih mejah EU. Na novembrskem zasedanju v Strasbourgu je širitev potrdil tudi Evropski parlament. 6. decembra 2007 so notranji ministri EU sprejeli dokončno odločitev o širitvi schengenskega območja.

21. decembra 2007 se je ob polnoči zgodila širitev schengenskega območja na devet novih članic EU, tudi Slovenijo. S tem je bil odpravljen nadzor na kopenskih in morskih notranjih mejah. 30. marca 2008 je bil odpravljen tudi nadzor na zračnih notranjih mejah.

2.2.7 Schengen in sredstva EU

Schengenski standardi oz. njihovo uvajanje v vsaki izmed članic povzročijo tudi veliko stroškov. Zato je bil z Aktom o pogojih pristopa novih članic ustanovljen Schengenski vir. To je bil začasni instrument za pomoč od dneva pristopa v EU do konca leta 2006. Do pomoči je bilo upravičenih 7 novink, med njimi tudi Slovenija, ki je dobila 119,8 milijona evrov. Namen te pomoči je financiranje ukrepov na novih zunanjih mejah EU. Med te ukrepe spadajo:

- naložbe v izgradnjo, obnovo ali posodobitev infrastrukture mejnih prehodov in drugih objektov na mejnih prehodih,
- naložbe v opremo za izvajanje nadzora (laboratorijska oprema, naprave za odkrivanje, strojna in programska oprema za SIS II, prevozna sredstva),
- usposabljanje mejnih enot,
- stroški za logistiko in obratovanje.

Poleg omenjenega vira so novim članicam na voljo tudi druga sredstva EU. Z odločbami Evropskega parlamenta in Sveta so bili ustanovljeni štirje skladi, ki sestavljajo okvirni program Solidarnost in upravljanje migracijskih tokov s področja svobode. Za obdobje 2007–2013 so za omenjeni program predvidena sredstva v znesku 4,02 milijarde evrov. Slovenija bo dobila cca. 64,8 milijonov evrov, razdeljeni pa bodo med naslednje sklade:

- Evropski sklad za vključevanje državljanov tretjih držav za obdobje 2007–2013 (5,6 milijona evrov),
- Sklad za zunanje meje za obdobje 2007–2013 (47,2 milijona evrov),
- Evropski sklad za begunce za obdobje 2008–2013 (4,2 milijona evrov),
- Evropski sklad za vračanje za obdobje 2008–2013 (7,8 milijona evrov).

Namen teh skladov je zagotovitev enakomerne porazdelitve bremen med državami članicami pri upravljanju zunanje meje ter izvajanju skupne politike priseljevanja in azila. Finančni prispevek v okviru Sklada ima obliko donacij. Posamezni skladi so financirani s strani Skupnosti v višini 75 odstotkov.

2.2.8 Stroški SIS

Aplikacija SISone4all je bila vsem novim članicam ponujena brezplačno, za infrastrukturo pa so morale poskrbeti same države. V Sloveniji so bili dodatni stroški zaradi sistema SISone4all ocenjeni na 100.000 evrov.

V zadnji fazi pristopnih pogajanj je bil za nove članice potrjen vir sredstev, ki je bil namenjen za vzpostavljanje schengenskih standardov na zunanjih mejah. Sredstva so znašala milijardo evrov, Sloveniji je bilo namenjenih približno 119 milijonov evrov.

V tabeli 3 so prikazani izdatki za postavitve C.SIS, ki so nastali od 18. 12. 1991 do 31. 12. 2007.

Tabela 3: Podatki o večletnih odobrenih izdatkih za postavitve tehnične podporne funkcije C.SIS

Razčlenitev izdatkov	Znesek v EUR
C.SIS.I	
• Proračun, odobren za obdobje od 18. 12. 1991 do 31. 12. 2006	28.453.277,20
• Novi odobreni izdatki v letu 2007	2.678.050,74
Skupaj C.SIS.I	31.131.327,94
SIS II	
• Proračun, odobren do 31. 12. 2006	461.663,26
• Novi odobreni izdatki v letu 2007	0,00
Skupaj SIS II	461.663,26
Oba skupaj	31.592.991,20

Vir: Council of the European Union, 2008

V tabeli 4 so prikazani ocenjeni stroški pri postavitvi in obratovanju sistema C.SIS v letih 2008 in 2009.

Tabela 4: Predvideni stroški postavitve in obratovanja sistema C.SIS v letih 2008 in 2009 (v EUR)

	2008	2009
Stroški postavitve	2.370.000	2.030.000
Stroški obratovanja	2.625.000	2.525.000
Skupaj	4.995.000	4.555.000

Vir: Council of the European Union, 2007 in Council of the European Union, 2008

2.2.9 Zgodovina Schengenskega sporazuma

Že pred prvo svetovno vojno se je dalo brez potnega lista potovati od Pariza v Franciji do Sankt Peterburga v Rusiji. Z začetkom vojne te svobode gibanja ni bilo več, so se pa pozneje vzpostavila določena območja, kjer je bilo to spet mogoče.

Leta 1922 se je Irska odcepila od Združenega Kraljestva, vendar državi nista zahtevali potnega lista za prehod meje.

Leta 1954 so dogovor o ukinitvi medsebojnih meja podpisale nordijske države Danska, Finska, Norveška in Švedska. V veljavo je stopil leta 1958. Istega leta so podoben medsebojni dogovor podpisale države Beneluksa. Slednji je stopil v veljavo dve leti pozneje.

Dogovor o postopni ukinitvi medsebojnih meja sta podpisali tudi Francija in Nemčija, in sicer leta 1984.

Schengenski sporazum je bil na začetku neodvisen od EU. Delno zaradi nesoglasja med članicami EU, delno pa zato, ker države, ki so bile pripravljene na uvedbo schengena, niso hotele čakati drugih. Tako so leta 1985 sporazum podpisale Nemčija, Francija, Nizozemska, Belgija in Luksemburg. Pet let kasneje je bila podpisana tudi konvencija o izvajanju sporazuma. Oba dokumenta sta bila podpisana na krovu ladje Princesse Marie–Astrid v kraju Schengen, na tromeji med Nemčijo, Francijo in Beneluksom.

2.3 Pruemska pogodba (SIS III)

Pruemska pogodba, ki je poznana tudi kot SIS III, je bila podpisana 27. maja 2005 v Pruemu v Nemčiji. Države podpisnice so bile Nemčija, Španija, Francija, Luksemburg, Nizozemska, Avstrija in Belgija. Namen pogodbe je okrepitev čezmejnega policijskega sodelovanja, zlasti na področju boja proti terorizmu, čezmejnemu kriminalu in nezakoniti migraciji.

Pomen pogodbe je še toliko večji, saj so v njej bistveno izboljšani in učinkovito organizirani postopki za izmenjavo informacij. Sodelujoče države bi tako lahko druga drugi omogočile samodejni dostop do posebnih nacionalnih podatkovnih baz.

Države pogodbenice bi imele neomejen in neposreden spletni dostop s polno pravico branja podatkov v registrih motornih vozil držav partnerk. Druga drugi bi omogočile dostop do podatkovnih baz analiz DNK in baz prstnih odtisov v okviru t. i. sistema za iskanje zadetkov. Policija bi lahko sprožila iskanje v podatkovnem sistemu v kateri koli izmed držav pogodbenic in tako izvedela, ali vsebuje podatke o določenem profilu, o rezultatih pa bi bila samodejno obveščena v nekaj minutah. Nadaljnje informacije, kot so osebni podatki, bi se lahko sporočale v okviru medsebojne pravne pomoči.

Poleg navedenega Pruemska pogodba predvideva izmenjavo podatkov o morebitnih teroristih in huliganih. Z operativnimi ukrepi, kot so skupne patrolje, bi se lahko okrepilo tudi policijsko sodelovanje, pri čemer bi se javna pooblastila prenesla na policijske sile drugih držav pogodbenic. Okrepila bi se lahko tudi pomoč v primeru dogodkov velikih razsežnosti.

V Sloveniji je pogodba stopila v veljavo 8. avgusta 2007.

2.4 Vizumski informacijski sistem (VIS)

VIS je še ena izmed baz podatkov. V njej se bodo zbirali fotografije in prstni odtisi vseh prosilcev za izdajo schengenskega vizuma. Poleg biometričnih in osebnih podatkov o prosilcu se bodo zbirali tudi podatki o kraju in datumu predložitve vloge za izdajo vizuma ter odločitev države članice, pristojne za izdajo, podatki o odobritvi ali zavrnitvi izdaje, oziroma preklicu ali podaljšanju veljavnosti vizuma.

Prav tako kot SIS je tudi VIS sestavljen iz nacionalnega (CS-VIS) in nacionalnega dela (NI-VIS).

Sistem je bil ustanovljen junija 2004, operativen pa naj bi bil spomladi 2009. Ko bo dokončan, bo vanj vsako leto vnesenih približno 20 milijonov podatkov. Glede na to, da bodo podatki v sistemu hranjeni do pet let, bo to največja podatkovna baza na svetu.

Namen sistema VIS je olajšati izmenjavo podatkov o vlogah za izdajo vizumov med državami članicami. S sistemom so tudi poenostavljeni postopki za pridobitev vizumov, preprečeval pa naj bi trgovanje z vizumi in pripomogel v boju proti goljufijam ter olajšal preverjanje na zunanjih mejnih prehodih Unije. VIS bi moral pripomoči tudi k ugotavljanju istovetnosti oseb, ki ne izpolnjujejo pogojev za vstop, začasno ali stalno prebivanje na ozemlju držav članic, in prispevati k preprečevanju groženj notranji varnosti katere koli države članice.

Dostop do podatkov bi moral biti vedno zabeležen in mogoč le ob posebnih, točno določenih pogojih. Zbirko podatkov bo upravljal stalni upravljavski organ, ki bo zbiral informacije iz vseh članic schengenskega območja. Do podatkov bodo lahko dostopali le pooblaščenim uslužbenci nacionalnih organov za izdajo vizumov, mejni nadzor, priseljevanje, azil in notranjo varnost ter le za namene nadzora meje, preverjanje prošnje za azil ali druge, zelo omejene namene, določene z uredbo.

Drugi preiskovalni organi držav članic in Europol bodo lahko dostopali do podatkov le v posebnih primerih za preprečevanje terorističnih in drugih hudih kaznivih dejanj, vendar ob predhodni utemeljeni zahtevi. Samo v izjemnih nujnih primerih bodo lahko prošnje dane tudi ustno in se bo njihova utemeljenost preverjala kasneje. Tudi posredovanje podatkov tretjim državam naj bi bilo dovoljeno samo v izjemnih nujnih primerih in le s soglasjem države članice, ki je vnesla podatke.

Dostop do sistema za iskanje podatkov v namen preprečevanja, odkrivanja in preiskovanja terorističnih dejanj ter drugih hudih kaznivih dejanj bo podrobneje urejal tudi sklep, ki predvideva omejitve samo za tiste osebe, ki imajo ustrezna znanja o varovanju podatkov ter ob ustreznih odobritvah. Nacionalni organi bodo morali pripraviti seznam točk za dostop, iskanje podatkov pa bo mogoče le na podlagi utemeljene razlage, da bo res bistveno pripomoglo pri preiskavi hudih kaznivih dejanj.

Podobno, kot določa uredba o dostopu do VIS, bo moralo iskanje podatkov potekati ob izpolnjevanju točno določenih pogojev. Njihovo posredovanje tretjim državam bo dovoljeno le v izjemnih primerih.

2.5 Eurodac

EURODAC je evropska podatkovna zbirka prstnih odtisov. Njen namen je vzpostavitev sistema za identifikacijo prosilcev za azil ter ilegalnih priseljencev, s čimer se bo poenostavila aplikacija uredbe Dublin II, ki omogoča določitev države članice, ki je odgovorna za obravnavo vloge za dodelitev azila.

Vsem prosilcem za azil in ilegalnim priseljencem s starostjo nad 14 let se sedaj v rutinskem postopku odvzamejo prstni odtisi. Prstni odtisi so posredovani osrednji enoti znotraj Evropske komisije, kjer se opravi avtomatska primerjava s prstnimi odtisi, ki so v podatkovni zbirki. Tako se potem vidi, če je prosilec vstopil v EU brez potrebnih dokumentov in če je za azil zaprosil že v kateri drugi članici EU. Sistem deluje od 15. januarja 2003 in je prvi tovrstni sistem v EU.

Sistem pospešuje obravnavanje vlog za azil, saj osebe preusmerja v državo, ki bi morala obravnavati vlogo. Poleg tega prosilcem za azil preprečuje, da bi v primeru zavrnitve v eni izmed članic, za azil prosili v drugi državi članici.

Če se prstni odtisi že nahajajo v bazi podatkov, se prosilca vrne v državo, kjer je prvotno zaprosil za azil. Če odtisov v bazi ni, prošnjo rešuje država, ki je odtise preverjala.

V Eurodac so vgrajeni ukrepi za varstvo človekovih pravic in državljskih svoboščin. Odtisi se uporabljajo le kot pomoč pri azilnem postopku in ne vsebujejo nobenih dodatnih osebnih podatkov. Shranjeni so do deset let, po preteku tega obdobja pa so avtomatsko izbrisani. Odtisi so izbrisani tudi v naslednjih primerih: ko prosilec pridobi dovoljenje za bivanje, zapusti območje države članice ali pridobi državljanstvo države članice.

2.6 Next Generation Identification

Next Generation Identification (NGI), Identifikacija naslednje generacije, je projekt ameriškega preiskovalnega urada FBI. Sedaj je sicer še vedno v uporabi Integrirani avtomatizirani sistem za identifikacijo na osnovi prstnih odtisov (IAFIS⁵), ki ima v podatkovni bazi več kot 60 milijonov oseb in je kot tak največja biometrična podatkovna baza na svetu. V bazo se v povprečju vnese od 9000 do 10000 oseb dnevno. IAFIS lahko vsebuje tudi podobo obraza.

⁵ Integrated Automated Fingerprint Identification System

NGI bo razširil zmožnosti sedanjega sistema, poleg prstnih odtisov pa bo lahko vseboval tudi odtis dlani, podatke o šarenici in podobo oblike obraza.

3 Biometrični potovalni dokumenti

Z biometričnimi potovalnimi dokumenti označujemo tiste potovalne dokumente, ki imajo vstavljen brezkontaktni čip z biometričnimi podatki o lastniku dokumenta. Brezkontaktni čip omogoča, da čitalec prebere podatke iz dokumenta brez fizičnega stika z dokumentom. Slika 5 prikazuje oznako, s katero se označuje biometrične potne liste. Oznaka se nahaja na platnici potnega lista.

Slika 5: Oznaka za biometrični potni list



Vir: Biometric passport, 2009, Wikipedia, The Free Encyclopedia

Standarde za biometrične potne listine so začeli razvijati v Mednarodni organizaciji za civilno letalstvo ICAO pred več kot 20 leti, leta 1986. Do leta 2010 naj bi vse države, ki so članice te organizacije, začele izdajati potne listine z brezkontaktnimi čipi.

Zaradi terorističnih napadov 11. 09. 2001 so ZDA sprejele številne ukrepe za obrambo pred teroristi. Eden izmed ukrepov je bil ustanovitev Ministrstva za domovinsko varnost, program za nadzor meje US-VISIT⁶. Program predvideva zbiranje biometričnih podatkov vseh oseb, ki za obisk ZDA potrebujejo vizum.

Za države, katerih državljani ne potrebujejo vizumov, so bile uvedene drugačne zahteve. Gre za države, ki so podpisale program za opustitev viz (Visa Waiver Program). Za ohranitev brezviznega statusa so morale te države do 26. 10. 2005 uvesti strojno berljive potne liste z digitalizirano fotografijo, najpozneje do 26. 10. 2006 pa tudi potne liste z biometričnimi podatki.

Svet EU je januarja 2005 sprejel Uredbo 2252/2004, ki določa varnostne značilnosti in biometrične podatke v potnih listih za države članice. V veljavo je stopila 18. 01. 2005. Določa, da morajo imeti potni listi držav članic EU vgrajen čip z zadostno kapaciteto, na katerem bosta shranjena zapisa podobe obraza in prstnih odtisov v interoperabilni obliki. Rok za implementacijo obrazne podobe je bil 18 mesec, za prstna odtisa pa 36 mesecev po sprejetju tehničnih specifikacij.

⁶ United States Visitor and Immigrant Status Indicator Technology

Dokument temelji na mednarodnih standardih, zlasti ISO standardih in ICAO priporočilih o strojno berljivih potovalnih dokumentih. Sprejema:

- zahteve za biometrične identifikatorje: obraz in prstni odtisi,
- pomnilniški medij (čip),
- logično podatkovno strukturo na čipu,
- zahteve za varnost digitalno shranjenih podatkov na čipu,
- ugotavljanje skladnosti čipov in aplikacij,
- RF združljivost z drugimi elektronskimi potovalnimi dokumenti.

Tehnične specifikacije so natančneje določene v Odločbi Komisije z dne 28. 06. 2006 (Komisija Evropskih skupnosti, 2006).

3.1 Skladnost s standardi

Potni listi Slovenije in ostalih držav EU ustrezajo več standardom in priporočilom:

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents (Vključitev biometričnih podatkov v strojno berljive potovalne dokumente), tehnično poročilo, različica 2.0, 5. maj 2004 [ICAO Bio];
- ISO/IEC 19794-5:2005: Formati izmenjave biometričnih podatkov – 5. del: Podatki podobe obraza;
- ISO/IEC 19794-4:2005: Formati izmenjave biometričnih podatkov – 4. del: Podatki podobe prstnega odtisa;
- ISO/IEC 14443: Identifikacijski dokumenti – Brezkontaktna kartica z integriranim(-i) vezjem(-i) – Kartice za branje z neposrednim približevanjem čitalniku;
- ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents (Uporaba brezkontaktnih kartic z integriranim vezjem v strojno berljivih potovalnih dokumentih), tehnično poročilo, različica 3.1, 16. april 2003;
- International Civil Aviation Organization (ICAO) (Mednarodna organizacija civilnega letalstva), Machine Readable Travel Documents (Strojno berljivi potovalni dokumenti), dokument 9303, del 1 Machine Readable Passports (Strojno berljivi potni listi), osnutek šeste izdaje, 2006;
- ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies (Razvoj logične podatkovne strukture – LDS za tehnologije za izbirno povečanje zmogljivosti), tehnično poročilo, revizija 1.7, 18. maj 2004;
- ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access (IJK za strojno berljive potovalne dokumente, ki dopušča bralni dostop ICC), tehnično poročilo, različica 1.1, 1. oktober 2004;
- ISO/IEC 7816-4:2005, Identifikacijski dokumenti – Kartice z integriranim vezjem – 4. del: Organizacija, varovanje in ukazi za izmenjavo;

- Advanced Security Mechanisms for Machine Readable Travel Documents (Napredni varnostni sistemi za strojno berljive potovalne dokumente), različica 1.0, 2005;
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application" (Varnostni profil na podlagi skupnih meril za strojno berljive potovalne dokumente z „aplikacijo ICAO“), Basic Access Control (Osnovni nadzor dostopa), različica 1.0;
- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information" (standard „Format podatkov za izmenjavo informacij o prstnih odtisih, obrazu, brazgotinah in tetovažah (SMT)“) FBI: Wavelet Scalar Quantization (Valčna skalarna kvantizacija) (WSQ);
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application" (Varnostni profil na podlagi skupnih meril za strojno berljive potovalne dokumente z „aplikacijo ICAO“), Extended Access Control (Razširjeni nadzor dostopa), različica 1.0;
- Bruseljska skupina za interoperabilnost, obseg pooblastil;
- ICAO NTWG, RF Protocol and Application Test Standard for E-Passport (Protokol RF in testni standard za aplikacijo za elektronske potne liste); dela 2&3;
- ISO/IEC 7816-8: Identifikacijski dokumenti – Kartice z integriranim vezjem 8. del: Ukazi za varnostno delovanje.

3.2 Slovenski potni list

V Sloveniji so nove potne liste začeli izdajati 28. 08. 2006. V prvi fazi je na čipu shranjena samo podoba obraza, najpozneje 28. 06. 2009 pa se bodo začeli izdajati potni listi z dodanima prstnima odtisoma. Pri že izdanih biometričnih potnih listih se bodo prstni odtisi dodali naknadno. Stari potni listi ostajajo veljavni do njihovega poteka.

Novi potni listi se na pogled bistveno ne razlikujejo od starih. Na platnici potnega lista je posebna mednarodno dogovorjena oznaka, ki nakazuje, da dokument vsebuje čip. Čip je nevidno vgrajen v polikarbonatni strani potnega lista z osebnimi podatki, ki je zato nekoliko debelejša in tudi bolj trdna. Oblikovna podoba potnih listov se od stare razlikuje tudi po barvnem odtenku strani potnega lista. Modro-rdečo barvo so zamenjali modro-zeleni odtenki; izbor motivov, ki predstavljajo osnovne kulturne in zgodovinske informacije oz. značilnosti Slovenije, pa ostaja enak. Kot zahteva EU, so na obrazcih potnega lista določeni podatki napisani v vseh uradnih jezikih Evropske Unije. Napis Evropska unija je dodan tudi na platnico potnega lista.

3.2.1 Čip

Najpomembnejša novost v novem potnem listu je integrirani čip za shranjevanje podatkov. Zaradi varnosti in tudi količine podatkov, ki so shranjeni (fotografija, prstna odtisa, osebni

podatki, kriptografski elementi ...), se je kot najbolj primeren medij izkazal brezkontaktni pametni čip.

V slovenskem biometričnem potnem listu je vgrajen Philipsov SmartMX brezkontaktni čip s pomnilnikom velikosti 72K ter Gemalto operacijskim sistemom.

Philipsovi oz. NXP čipi (NXP je podružnica podjetja Philips) so danes daleč najbolj uporabljeni čipi – najdemo jih v 80 % biometričnih potnih listov.

Zapis na čipu bo v standardni obliki, imenovani Logična struktura podatkov (LDS⁷), ki zagotavlja interoperabilnost, kar pomeni, da so potni listi berljivi s katero koli strojno in programsko opremo, ki jo imajo mejni organi. Maja 2003 je bilo izdano poročilo, v katerem so podane smernice in nasveti državam, kako uporabiti infrastrukturo javnih ključev (IJK) – infrastrukturo za zagotavljanje varnosti pri strojno berljivih potovalnih dokumentih. Med pomembnejše tehnične zahteve spadajo še: območje berljivosti do 10 cm, LDS mora biti izveden z metodo naključnega dostopa, čipi morajo ustrezati predpisom ISO 14443 tipu A ali tipu B.

NXP čip popolnoma ustreza specifikacijam, ki jih je podala ICAO, v marsičem pa jih tudi presega.

3.2.2 Podatki na čipu

Običajni potni list ima poleg podatkov o lastniku in fotografije tudi dve vrstici strojno berljivih podatkov (MRZ⁸), ustrezati pa mora tudi fizičnim varnostnim standardom.

MRZ se nahaja na levem robu – vrstici imata po 44 znakov in vsebujeta med drugim ime in priimek lastnika, njegov rojstni datum in številko potnega lista.

Čip poleg MRZ vsebuje še biometrične podatke in elemente za digitalno zaščito podatkov na njem. Podatki na čipu so razvrščeni v 16 skupin.

Prvo skupino predstavlja MRZ. V drugi skupini se nahaja slika obraza v formatu jpeg2000, v tretji (DG3) prstni odtis in v četrti slika šarenice. Zaenkrat sta na čipih potnih listov evropskih držav in ZDA samo prvi dve skupini – MRZ in slika. V naslednji fazi bosta dodana tudi prstna odtisa obeh kazalcev, obenem pa se bo dogradil sistem zaščite podatkov na čipu.

⁷ Logical Data Structure

⁸ Machine Readable Zone

3.2.3 Zaščita podatkov na čipu

Poleg podatkov o imetniku na čipu najdemo "varnostni objekt" (SO_D⁹), v katerem so digitalno podpisani povzetki vseh skupin podatkov, ki so na čipu. Za digitalni podpis je uporabljen zasebni ključ podpisnika dokumentov (DS¹⁰). Podpisniku dokumentov izda digitalno potrdilo državni overitelj (CSCA¹¹). Vsaka država, ki na podlagi teh specifikacij izdaja biometrične potne liste, je morala ustanoviti posebnega izdajatelja digitalnih potrdil za biometrične potne listine. V Sloveniji je to CSCA-SI, ki izdaja potrdila DS. Z DS upravlja Ministrstvo za notranje zadeve kot naročnik potnih listov, nameščen pa je v podjetju Cetus, ki potne liste izdeluje. Potrdilo DS je zapisano tudi na čipu, s čimer se nadzornim sistemom na mejah olajša preverjanje.

Pri potnih listih prve generacije (brez prstnih odtisov) se uporabljata dve vrsti zaščite:

- osnovni nadzor dostopa (angl. *Basic Access Control* – BAC)
Kontrolor pri preverjanju odprt potni list položi na optični čitalec, ki prebere MRZ in ga sporoči terminalu. Slednji iz MRZ izračuna ključ za simetrični algoritem trojni DES. Če izračunan ključ ni pravi, dostop do podatkov ni dovoljen. S tem ukrepom naj bi preprečili, da bi poljubni čitalec prebral podatke na čipu. Ker MRZ ob zaprtem potnem listu ni viden, se sklepa, da je imetnik svoj potni list prostovoljno izročil v pregled. Ta kontrola, ki je sicer obvezna po odločbi Evropske komisije, ne more preprečiti, da bi čip kopirali.
- pasivna avtentikacija (angl. *Passive Authentication*)
Na čipu se nahaja javni ključ podpisnika, s katerim terminal preveri digitalni podpis SO_D. To stori tako, da ugotovi, ali je bilo potrdilo izdano od ustreznega državnega overitelja. Digitalna potrdila CSCA niso javno dostopna, države si jih med seboj izmenjajo po diplomatski poti. Za spremembo podatkov na čipu je torej treba poznati zasebni ključ podpisnika (izdelovalca potnih listov).

Ta način kontrole, ki je obvezna po dokumentu ICAO, dokazuje, da podatki na čipu niso bili spremenjeni. Ne prepreči pa, da bi čip kopirali ali nadomestili z drugim.

Pri potnih listih druge generacije (s prstnimi odtisi) so možne dodatne vrste zaščite:

- aktivna avtentikacija (Active Authentication)
Čipi vsebujejo poseben par asimetričnih ključev za aktivno avtentikacijo – javni ključ (v skupini podatkov 15 – DG15) in zasebni ključ (v zaščitenem delu spomina). Zasebnega ključa se ne da prebrati, uporablja pa se v internih operacijah. V primeru zamenjave tega para ključev bi to odkrili pri pasivni avtentikaciji, saj je povzetek javnega ključa vključen v SO_D. Čip dobi od terminala v podpis naključno generirano

⁹ Document Security Object

¹⁰ Document Signer

¹¹ Country Signing Certificate Authority

število in z uporabo ključa v DG15 preveri, da je odgovor res podpisan z zasebnim ključem čipa. To dokazuje, da čip ni bil kopiran ali nadomeščen z drugim.

Slaba stran tega sistema je, da se ga lahko uporabi za sledenje osebam in kot tak predstavlja grožnjo zasebnosti.

- razširjeni nadzor dostopa (Extended Access Control – EAC)

Sestavljen je iz dveh kontrol, ki bosta za potne liste držav EU obvezni najkasneje od 28. junija 2009, ko bodo na čipu prstni odtisi:

— avtentikacija čipa (Chip Authentication)

Javni ključ se v tem primeru nahaja v skupini podatkov 14 (DG14). Ta sistem kontrole nadomešča aktivno avtentikacijo – prednost tega sistema je v tem, da pri vzpostavitvi komunikacije z nadzornim sistemom čip ne podpiše poslanega sporočila, poleg tega pa je zagotovljena močna enkripcija za dostop do občutljivih podatkov na čipu.

— overjanje terminala (Terminal Authentication)

Čip dovoli povezavo samo nadzornim sistemom (IS, angl. *Inspection Systems*), ki imajo poleg digitalnega potrdila sistema za preverjanje dokumentov (DV, angl. *Document Verifier*) tudi pripadajoči zasebni ključ. Sistemom za preverjanje dokumentov potrdilo izda državni overitelj CVCA (angl. *Country Verifying Certificate Authority*).

Države bodo tako morale poleg CSCA vzpostaviti še eno infrastrukturo javnih ključev za nadzorne sisteme – državno CVCA, ki bo izdajala potrdila sistemom za preverjanje dokumentov, ti pa jih bodo izdajali posameznim nadzornim sistemom – terminalom na mejah (IS). CVCA izdaja potrdila tudi DV drugih držav. Digitalno potrdilo državne CVCA se shrani v zaščiteni del spomina čipa v fazi personalizacije.

Slovenski DV bo izdajal digitalna potrdila vsem slovenskim IS, obenem pa bo moral zase pridobiti digitalna potrdila od CVCA drugih držav in jih potem posredovati vsem slovenskim IS. Kot primer vzemimo, da se bo na mejni kontroli v Sloveniji pojavil državljan Avstrije. Čip na njegovem potnem listu bo od IS zahteval potrdilo, ki ga je DV Slovenije prejel od avstrijske CVCA. Ker čip v spominu vsebuje digitalno potrdilo avstrijske CVCA, lahko preveri, ali IS pozna potrdilo DV, ki je bilo izdano od avstrijske CVCA, in samo takim IS dovoli dostop do podatkov.

Potek izmenjav predstavlja določene težave, saj je treba zagotoviti interoperabilnost in neprekinjeno delovanje ustreznih strežnikov, poleg tega pa dodatno težavo predstavljajo digitalna potrdila, katerih veljavnost se ne pokriva z veljavnostjo potnih listov.

Zato je treba omogočiti, da čipi ob kontaktih z IS v kateri koli državi naložijo novo potrdilo matične CVCA, ko staro potrdilo preteče ali postane neveljavno.

1. novembra 2007 je Nemčija začela izdajati biometrične potne liste druge generacije, ki imajo v čipu shranjeno tudi podobo prstnih odtisov. Po novem je drugačen tudi dostop do čipa – preverjanje se izvrši v naslednjem vrstnem redu:

- osnovni nadzor dostopa,
- pasivno overjanje,
- overjanje čipa in
- overjanje terminala.

3.2.4 Ponarejanje biometričnih potnih listov

Kljub vsem kontrolam novi potni listi ne vzbujajo velikega zaupanja. Od začetka leta 2006 lahko spremljamo novice, da je posameznikom uspelo potne liste "razbiti".

3.2.4.1 Nemški potni list

Leta 2006 je Lukas Grunwald, nemški svetovalec za računalniško varnost, uspel klonirati biometrični potni list. To mu je uspelo v samo dveh tednih. Večino časa je porabil za prebiranje standardov za biometrične potne liste, ki so objavljeni na spletni strani Mednarodne organizacije za civilno letalstvo (ICAO). Napad je izvedel na nemški potni list, vendar bi metoda učinkovala na potnem listu katere koli države, saj so standardi povsod enaki.

Na demonstraciji, ki jo je uprizoril za spletno stran Wired news, je potni list položil na RFID čitalec. Uporabil je uradni čitalec, kakršnega uporabljajo tudi na mejnih kontrolah. Čitalec je naročil direktno od proizvajalca čitalcev, vendar je dejal, da bi ga lahko izdelal tudi sam, tako da bi na standardni čitalec dodal anteno.

Zagnal je program Golden Reader Tool (slednjega za branje potnih listov uporabljajo tudi na mejah) in po štirih sekundah so se podatki na čipu prikazali na zaslonu. Na čitalec je nato položil prazno vzorčno stran potnega lista s praznim RFID čipom in jo priredil ICAO ureditvi, tako da je osnovna struktura ustrezala tisti na pravem potnem listu.

S programom RFDump, ki ga je s kolegom razvil pred leti, je podatke s čipa na potnem listu prenesel na računalnik, nato pa novi čip programiral s kopiranimi podatki. Tako je dobil prazen dokument, ki pa je s stališča čitalca enak originalnemu dokumentu.

Šel pa je še korak dalje. Potni list oz. čip je kloniral na čip pametne kartice, ki jo je prej formatiral v ICAO standardu. Čitalec je nato ukanil tako, da je med čip na potnem listu in čitalec vstavil pametno kartico. Ker je čitalec zasnovan tako, da lahko naenkrat prebere samo en čip, prebere tisti čip, ki mu je bliže.

To pomeni, da bi lahko nekdo, ki je na seznamu iskanih oseb, imel pri sebi svoj pravi potni list, vendar s čipom, ki je bil kloniran z drugega potnega lista. Taka ukana bi sicer uspela samo na računalniku, ki se zanaša na elektronske informacije in ne na podatke, ki so zapisani na potnem listu.

Odgovor na Grunwaldovo kloniranje čipa je bil, da je v specifikacijah navedeno, da čip ni zaščiten pred kopiranjem, to pa naj bi se spremenilo, ko bo uveden razširjeni nadzor dostopa (EAC). Problem pri EAC je v tem, da ne gre za mednarodni standard, saj ga ni pripravil ICAO, temveč nemški BSI (nem. *Bundesamt für Sicherheit in der Informationstechnik*). Zaradi tega EAC ni obvezen za vse države, zato konzorcij FIDIS (angl. *Future of Identity in the Information Society*) opozarja, da bi bilo potrebno razviti nov varnostni koncept, ki bi veljal po celem svetu.

S kopiranjem pa Grunwald ni naredil veliko, saj je za kopiranje potrebno posedovanje potnega lista. Če bi ponarejevalec imel dostop do tujega potnega lista, bi ga lahko tudi ukradel. Res pa je, da pravi lastnik v primeru kraje potni list prekliče.

Lahko bi se zgodilo, da bi na primer receptor v hotelu kopiral čip – lastnik potnega lista tega ne bi vedel in bi po odhodu iz hotela dobil potni list nazaj. V tem primeru lastnik potnega lista ne bi preklical, vendar bi lastnik ponarejenega potnega lista za njegovo uporabo moral biti fizično zelo podoben pravemu lastniku.

Za resnično »razbitje« potnega lista bi bilo treba čip klonirati, nato pa na njem spremeniti podatke, kar pa ni možno, saj kontrola BAC odkrije spremembo, kar je priznal tudi Grunwald.

Pozneje je Grunwaldu uspel nov poskus – dokazal je, da se da čip prirediti tako, da pri skeniranju napade čitalec. Uspelo mu je sabotirati dva čitalca različnih proizvajalcev tako, da je kloniral čip, nato pa modificiral slikovno datoteko v JPEG2000 formatu, ki vsebuje sliko imetnika.

Na tak način bi se dalo na čip zapisati zlonamerno kodo, s pomočjo katere bi prišlo do tega, da bi ob napadu čitalec odobril potni list, čeprav bi bil ta ponarejen ali imel pretečen rok.

3.2.4.2 Britanski potni list

Podoben napad kot Lukas Grunwald sta na britanski potni list izvedla Steve Boggan, novinar britanskega časopisa *The Guardian*, in Adam Laurie, računalniški strokovnjak in varnostni svetovalec v podjetju *The Bunker Secure Hosting*.

Tako kot Grunwald je tudi Laurie na spletni strani organizacije ICAO našel vse potrebne informacije. Med drugim tudi to, da je ključ za dostop do podatkov na čipu sestavljen iz številke potnega lista, datuma rojstva lastnika in datuma poteka dokumenta.

Kljub uporabi enkripcijskega algoritma 3DES, ki zagotavlja visoko stopnjo zaščite, je bilo prekršeno eno izmed osnovnih načel enkripcije, saj je ključ do čipa razviden iz MRZ.

Ampak tudi v tem primeru je bil komentar, da so na čipu samo podatki, ki so tako ali tako vidni v potnem listu.

Med tehnične težave spada tudi razdalja, s katere čitalec lahko prebere čip. Ta naj bi znašala do 2 cm, vendar naj bi na Nizozemskem uspeli čip prebrati tudi z razdalje 30 cm. Laurie je sestavil napravo, ki je zaznala potni list na razdalji 7,5 cm, kar je dovolj, da bi nekdo, ki sedi poleg nas, npr. na avtobusu, skeniral naš potni list. Za vzpostavitev povezave s čipom je resda potreben vpogled v potni list, vendar je Laurie predvidel naslednji scenarij: poštar, ki naj bi dostavil potni list, bi lahko prišel do podatkov na čipu, ne da bi odprl kuverto. Kot že rečeno, za to rabi tri podatke. Rojstni datum že pozna, saj so med pošto tudi rojstnodnevne voščilnice, datum izteka potnega lista pa je približno 10 let od včerajšnjega dneva. Ostane samo še devetmestna številka potnega lista. Član skupine NO2ID, ki je prisostvoval pri poskusu, je dejal, da se po poročanju 30 000 članov skupine v prvih štirih znakih kaže precej podobnosti, tako da je potrebno ugotoviti samo še zadnjih pet števil. Če bi poštar potni list odnesel domov, bi lahko v manj kot enem dnevu s preskušanjem vseh možnosti ugotovil še manjkajoči podatek in tako prišel do podatkov na čipu. Potni list bi bil tako dostavljen samo dan pozneje.

Ta način je izvedljiv, saj je omogočen sistematičen poskus vseh možnosti. Če bi bilo število napačnih poskusov omejeno, bi bil tak način dostopa do čipa pravzaprav nemogoč.

3.2.4.3 Nizozemski potni list

Podoben primer kot z britanskim poštarjem je bil ugotovljen tudi na Nizozemskem. Pri izmenjavi podatkov med čitalcem in potnim listom so bili podatki prestreženi in shranjeni, dostopno geslo pa je bilo ugotovljeno v manj kot dveh urah. Ker so bili potni listi izdani po zaporednih številkah, je bil dostop do gesla še toliko hitrejši.

3.2.4.4 Testiranje v podjetju Flexilis

V podjetju Flexilis iz ZDA so pri prototipu ameriškega biometričnega potnega lista ugotovili dodatno pomanjkljivost. Potni list v sprednji platnici vsebuje zaščito, ki preprečuje, da bi potni list skenirali z večje razdalje.

Kot so Kevin Mahaffey in ostala ekipa iz Flexilisa ugotovili, je ta zaščita učinkovita samo, če je potni list popolnoma zaprt. Če je odprt, pa čeprav gre samo za nekaj milimetrov, kar se lahko zgodi, če je potni list v žepu ali torbi, zaščita ne deluje več.

Zaradi BAC je dostop do podatkov na čipu sicer onemogočen, je pa možno na tak način na daljavo zaznati prisotnost potnega lista, kar predstavlja veliko grožnjo.

Kot rešitev je bila predlagana boljša zaščita potnega lista, ki bi bila vstavljena v obe platnici. Ta bi dovolila dostop do čipa, šele ko bi bil potni list precej bolj odprt.

V demonstraciji, kaj se lahko zgodi, če bi zaščita ostala taka, kot je, so v kanto za smeti namestili bombo, ki se je aktivirala, ko je čitalec zaznal prisotnost lutke z delno odprtim potnim listom. Test je bil ponovljen s poznim listom, ki je imel izboljšano zaščito, in do detonacije ni prišlo.

Video posnetek testiranja je dostopen na naslovu <http://www.youtube.com/watch?v=-XXaqrF7pI>.

Podobno hibo so pri evropskih potnih listih odkrili Henning Richter iz Nemčije ter Wojciech Mostowski in Erik Poll iz Nizozemske.

Dokazali so, da je potni list moč zaznati, poleg tega pa je mogoče tudi določiti državljanstvo lastnika oz. lastnice potnega lista. Za razliko od ameriških potnih listov evropski v platnicah ne vsebujejo ščita.

Test je bil uspešno izveden na potnih listih desetih držav, čeprav bi to pomanjkljivost verjetno našli tudi v drugih potnih listih z BAC. Čeprav vsi potni listi ustrezajo istemu standardu, so med njimi kljub vsemu določene razlike.

Po standardu ISO 14443 je največja razdalja, s katere čitalec lahko prebere čip, 10 cm, pri običajno uporabljenih čitalcih pa je ta razdalja od 1 do 2 cm. Kljub temu so možne tudi večje razdalje. Prisluskovanje povezavi med čipom in čitalcem je možno tudi z oddaljenosti devetih metrov.

Standard definira določene ukaze in ustrezne odgovore. Na ukaze, ki niso definirani, se potni listi različnih držav različno odzivajo in na podlagi teh odgovorov je možno določiti poreklo potnega lista.

Kot uspešen protiukrep bi se izkazalo, če bi ICAO v specifikacijah za nedefinirane ukaze predpisal standardne odgovore. To bi zelo otežilo ali celo onemogočilo določanje nacionalnosti. Kljub temu bi se na tak način še vedno dalo ugotoviti prisotnost potnega lista. Odpravo te pomanjkljivosti bi se doseglo z vstavitvijo kovinskega ščita v platnice, tako kot je to primer pri ameriških potnih listih.

Že omenjani Lukas Grunwald je uspel klonirati potni list, ni pa mogel spremeniti podatkov na kloniranem čipu, ne da bi bilo to neopaženo.

Pri tem poskusu je bil uspešen Jeroen van Beek, nizozemski varnostni raziskovalec z univerze v Amsterdamu.

S pomočjo čitalca, dveh čipov ter javne in lastne programske opreme je uspel kopirana čipa spremeniti in prilagoditi do stopnje, ko bi ju bilo treba samo še vstaviti v ponarejen ali ukraden potni list.

Prikaz je potekal tako, da je najprej s pomočjo čitalca in kode prišel do podatkov na čipu. To se sicer ne bi smelo zgoditi, ampak kako se to naredi, je že pred letom in pol pokazal Adam Laurie. Nato je podatke prenesel na drug čip, katerega je program Golden Reader Tool spoznal za originalnega. Vendar tudi to ni nič novega, saj je Lukasu Grunwaldu to uspelo že pred leti.

Jeroen van Beek je nato storil nekaj, kar do takrat ni uspelo še nikomur. Na kloniranimi čipoma je obstoječi sliki zamenjal s slikama Osame bin Ladna in Hibe Darghmeha, palestinskega samomorilskega napadalca, in če bi čip vseboval tudi druge biometrične podatke, bi z lahkoto spremenil tudi te. Program Golden Reader ne bi potrdil avtentičnosti čipa zaradi zapsanega in spremenjenega digitalnega podpisa. Vendar je s pomočjo programa CryptLib, ki ga je napisal Peter Gutmann iz Aucklandske univerze na Novi Zelandiji, ki ga je van Beek priredil, uspel programirati digitalni podpis, ki je ustrezal novemu potnemu listu in tako je bil ponarejen čip sprejet kot originalen.

Tako bi lahko kriminalci ustvarili potni list z lastnimi biometričnimi podatki ter imenom druge resnične osebe in potni list nemoteno uporabljali.

Tak način ponarejanja potnih listov se da odkriti s pomočjo imenika javnih ključev (PKD, angl. *Public Key Directory*), ki ga je vzpostavila organizacija ICAO. V tem primeru pride do preverjanja, ali se javni ključ potnega lista nahaja v PKD. Ker je novi digitalni podpis generiran z novim zasebnim ključem, temu pa ustreza novi javni ključ, ki ga v PKD ni. Pomanjkljivost sistema se kaže v tem, da prijava v sistem za države ni obvezna – od več kot 50 držav, ki izdajajo potne liste s čipom, je v imenik prijavljenih samo petina, med temi državami pa PKD dejansko uporablja samo polovica. Za učinkovito uporabo bi morale sodelovati vse države. Pri nekaterih državah je razlog to, da še niso pripravljene, pri drugih pa je možen razlog tudi to, da ne želijo posredovati digitalnih podpisov državam, ki jim ne zaupajo.

Ni pa PKD edini način za izmenjavo javnih ključev – nekatere države si jih med seboj izmenjujejo, vendar tudi to ni preveč uporabno, saj lahko ponarejevalci klonirajo potne liste držav, ki te izmenjave ne izvajajo.

Kljub vsemu je bila do sedaj uspešno opravljena sprememba podatkov samo na kloniranih čipih. Če bi podatke spremenili na pravih potnih listih, bi čitalec potni list takoj zavrnil. Res je, da so novi potni listi precej manj varni, kot je bilo pripovedovano, vendar so za ponarejevalce kljub vsemu še vedno trši oreh kot stari potni listi, saj je poleg knjižice dokumenta potrebno ponarediti tudi čip in digitalni podpis na njem.

3.3 Vrste potnih listov

Potne liste ureja Zakon o potnih listinah (ZPLD-1)¹², v katerem so našteje naslednje potne listine:

- potni list,
- diplomatski potni list,
- službeni potni list,
- potni list za vrnitev,
- potne listine, ki se izdajajo po mednarodni pogodbi.

Diplomatski potni list se izda predsedniku Republike Slovenije, poslancem Državnega zbora Republike Slovenije, poslancem iz Republike Slovenije v Evropskem parlamentu, predsedniku Državnega sveta Republike Slovenije, predsedniku in članom Vlade Republike Slovenije, predsedniku Ustavnega sodišča Republike Slovenije, varuhu človekovih pravic, predsedniku Vrhovnega sodišča Republike Slovenije, predsedniku Računskega sodišča Republike Slovenije, delavcem diplomatskih in konzularnih predstavništev ter misij Republike Slovenije v tujini, ki imajo diplomatske in konzularne nazive, ter delavcem ministrstva, pristojnega za zunanje zadeve, ki opravljajo diplomatske in konzularne zadeve ter imajo diplomatske nazive, vodjem državnih delegacij Republike Slovenije, osebam, ki po sklepu Vlade Republike Slovenije odhajajo na delo v mednarodne organizacije kot funkcionarji diplomatskega ranga v omenjenih organizacijah, diplomatskim kurirjem in določenim drugim osebam, če je to v interesu Republike Slovenije.

Diplomatski potni list se lahko izda tudi ožjim družinskim članom delavcev diplomatskih in konzularnih predstavništev ter misij Republike Slovenije v tujini in družinskim članom oseb, ki po sklepu vlade odhajajo na delo v mednarodne organizacije, če z njimi živijo v skupnem gospodinjstvu v tujini, ter ožjim družinskim članom oseb iz prejšnjega odstavka, če jih spremljajo na službeni poti v tujino.

Službeni potni list se izda svetnikom Državnega sveta Republike Slovenije, delavcem ministrstva, pristojnega za zunanje zadeve, in delavcem, zaposlenim v diplomatskih ali konzularnih predstavništvih Republike Slovenije v tujini, ki nimajo diplomatskega potnega lista.

Službeni potni list se izda tudi članom državnih delegacij Republike Slovenije in delavcem drugih državnih organov, kadar službeno potujejo v tujino, ter določenim drugim osebam, če je to v interesu Republike Slovenije.

Službeni potni list se lahko izda tudi ožjim družinskim članom oseb iz prvega odstavka tega člena, če z njimi živijo v skupnem gospodinjstvu v tujini.

¹² Uradni list RS, št. 3/2006 z dne 10. 01. 2006

Potni list za vrnitev je potna listina, ki se izda državljanu Republike Slovenije ali državljanu druge države članice Evropske unije, ki je v tujini ostal brez potne listine.

Potni list za vrnitev se izda državljanu druge države članice Evropske unije, če v državi, kjer je ostal brez potne listine, ni diplomatskega ali konzularnega predstavništva njegove države oziroma če tam njegova država ni kako drugače zastopana. Potni list za vrnitev se državljanu druge države članice Evropske unije izda le po pridobitvi soglasja pristojnega organa države, katere državljan je.

Sklep

Uporaba biometrije že dolgo dviga precej prahu. Zajemanje biometričnih vzorcev v biometričnih sistemih lahko pripelje do ogrožanja zasebnosti, saj bo s povečevanjem uporabe biometričnih sistemov možen nadzor gibanja vsakega posameznika. Predvsem bo ta nadzor v veliki meri omogočen, ko bo tehnologija toliko napredovala, da bo omogočeno zanesljivo prepoznavanje oseb prek nadzornih kamer. Ta nadzor ima tudi pozitivno stran – omogočeno bo tudi iskanje osumljenih oseb oz. nadzor nad njihovim gibanjem, kar bo znatno prispevalo k boju proti kriminalu in povečanju varnosti.

Vendar biometrija ter na drugi strani tudi digitalno podpisovanje prinašata varnost tudi na drugih področjih, kar je vzrok, da se uvajata v čedalje večjem številu poslovnih aplikacij (npr. e-bančništvo, e-uprava ...). Gre za sodoben način poslovanja, obenem pa tudi za edini način, ki zagotavlja, da je pri uporabi teh aplikacij uporabnik res tisti, za katerega se izdaja. Podobno velja tudi na področju potovalnih dokumentov. Biometrični potni listi »navadnim« uporabnikom omogočajo lažji prehod meja, med tem ko na drugi strani povzročajo težave tistim drugim, ki imajo nečiste namene.

Kljub vsemu je prostora za izboljšave in razvoj tako glede varnosti kot tudi glede zanesljivosti uporabe informacijske tehnologije pri potovalnih dokumentih (kot tudi na drugih področjih) še veliko. Gotovo je, da bodo na biometriji temelječi sistemi znatno vplivali na naše prihodnje življenje.

Literatura in viri

1. »Eurodac« system. Najdeno 16. januarja 2009 na spletnem naslovu <http://europa.eu/scadplus/leg/en/lvb/l33081.htm>
2. *A Trust Framework for ePassport Extended Access Control*. Najdeno 04. marca 2009 na spletnem naslovu http://download.entrust.com/resources/download.cfm/23409/WP_ePassport-EAC_May08.pdf?start
3. *Bioidentification*. (2009). Najdeno 10. januarja 2009 na spletnem naslovu <http://www.bromba.com/faq/biofaq.htm>
4. *Biometric passports*. (2009). Wikipedia, The Free Encyclopedia. Najdeno 10. januarja 2009 na spletnem naslovu http://en.wikipedia.org/wiki/File:EPassport_logo.svg
5. *Biometrics*. (2009). Wikipedia, The Free Encyclopedia. Najdeno 10. januarja 2009 na spletnem naslovu <http://en.wikipedia.org/wiki/Biometrics>
6. *Biometrija*. (2009a). Informacijski pooblaščenec. Najdeno 10. januarja 2009 na spletnem naslovu <http://www.ip-rs.si/varstvo-osebni-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/#c400>
7. *Biometrija*. (2009b). Wikipedija, prosta enciklopedija. Najdeno 10. januarja 2009 na spletnem naslovu <http://sl.wikipedia.org/wiki/Biometrija>
8. Boggan, S. (2006, 17. november). *Cracked it!* Najdeno 04. marca 2009 na spletnem naslovu <http://www.guardian.co.uk/technology/2006/nov/17/news.homeaffairs>
9. *Council of the European Union*. (2007). 14686/07. Najdeno 07. februarja 2009 na spletnem naslovu <http://www-securint.u-strasbg.fr/pdf/st14686.en07.pdf>
10. *Council of the European Union*. (2008). 15047/08. Najdeno 07. februarja 2009 na spletnem naslovu <http://register.consilium.europa.eu/pdf/en/08/st15/st15047.en08.pdf>
11. Damij, T. & Indihar Štemberger, M. (1995) *Uvod v poslovno informatiko in računalništvo*. Ljubljana: Ekonomska fakulteta.
12. *Dokumenti za prehod meje*. Najdeno 25. februarja 2009 na spletnem naslovu <http://www.policija.si/portal/organiziranost/uup/meja/dokumenti.php>
13. *E-passport security*. Najdeno 19. marca 2009 na spletnem naslovu https://www.os3.nl/2008-2009/epassport_eng
14. *ePassports EAC Conformity & Interoperability Tests*. Najdeno 19. marca 2009 na spletnem naslovu <http://www.e-passports2008.org/speakers-brauer-abstract>

15. Gradišar, M. & Resinovič, G. (1996). *Informatika v poslovnem okolju*. Ljubljana: Ekonomska fakulteta.
16. Gradišar, M., Jaklič, J., Damij, T. & Baloh, P. (2005). *Osnove poslovne informatike*. Ljubljana: Ekonomska fakulteta.
17. *Integrated Automated Fingerprint Identification System*. Najdeno 15. januarja 2009 na spletnem naslovu <http://www.fbi.gov/hq/cjisd/iafis.htm>
18. Kocbek, D. (2006, 25. oktober). *Frattini: Samo Slovenija je pripravljena*. Najdeno 31. januarja 2009 na spletnem naslovu <http://web.vecer.com/portali/vecer/v1/default.asp?kaj=3&id=2006102505124305>
19. Kocjan-Barle, M. & Bajt, D. (2003). *Slovenski veliki leksikon I: A–G*. Ljubljana: Mladinska knjiga.
20. *Komisija Evropskih skupnosti*. (2006). K 2006 (2909). Najdeno 16. marca 2009 na spletnem naslovu http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_s1.pdf
21. Lah, P. (2007, januar). *Biometrični potni list*. Najdeno 25. februarja 2009 na spletnem naslovu <http://www.ca.gov.si/kripto/kr-potnilist.htm>
22. Lettice, J. (2006, 30. januar). *Face and fingerprints swiped in Dutch biometric passport crack*. Najdeno 04. marca 2009 na spletnem naslovu http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack/
23. *Minister dr. Rupel na predstavitvi novih biometričnih potnih listov*. Najdeno 25. februarja 2009 na spletnem naslovu http://www.mzz.gov.si/index.php?id=13&tx_ttnews%5Btt_news%5D=11329&tx_ttnews%5BbackPid%5D=
24. *Neformalno zasedanje evropskih notranjih in pravosodnih ministrov*. Najdeno 31. januarja 2009 na spletnem naslovu <http://www.mnz.gov.si/nc/si/splosno/cns/novica/article/12027/5269/>
25. Ou, G. (2006, 09. avgust). *RFID passports with improper shielding triggers bomb in simulation*. Najdeno 04. marca 2009 na spletnem naslovu <http://blogs.zdnet.com/Ou/?p=289>
26. Ou, G. (2006, 18. december). *The ePassport cloning myth never dies*. Najdeno 04. marca 2009 na spletnem naslovu <http://blogs.zdnet.com/Ou/?p=394>
27. Ou, G. (2006, 21. avgust). *RFID passports and VeriChip security podcast*. Najdeno 04. marca 2009 na spletnem naslovu <http://blogs.zdnet.com/Ou/?p=301>

28. *Philips smart card chip technology secures France e-passports to meet global travel standards*. Najdeno 04. marca 2009 na spletnem naslovu http://www.nxp.com/news/content/file_1242.html
29. Poll, E. *Fingerprinting Passports*. Najdeno 25. februarja 2009 na spletnem naslovu http://www.cs.ru.nl/~erikpoll/talks/NLUUG_passport.pdf
30. *Poročilo o osnutku uredbe Sveta o migraciji s schengenskega informacijskega sistema (SIS I+) na drugo generacijo schengenskega informacijskega sistema (SIS II)*. Najdeno 07. februarja 2009 na spletnem naslovu <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2008-0352+0+DOC+XML+V0//SL>
31. Reid, D. (2006, 15. december). *ePassports 'at risk' from cloning*. Najdeno 04. marca 2009 na spletnem naslovu http://news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm
32. Rožič, B. (2006, 16. september). *Tehnični razlogi ovirajo SIS II*. Najdeno 20. januarja 2009 na spletnem naslovu http://www.dnevnik.si/tiskane_izdaje/dnevnik/201126
33. *Schengen Information System II (SIS II)*. Najdeno 07. februarja 2009 na spletnem naslovu <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/49.pdf>
34. *Sloveniji iz sklada za zunanje meje 47 milijonov evrov*. Najdeno 12. februarja 2009 na spletnem naslovu http://www.siol.net/eu/novice/2008/12/sloveniji_iz_sklada_za_zunanje_meje_47_milijonov_evrov.aspx
35. *Solidarnost in upravljanje migracijskih tokov*. Najdeno 12. februarja 2009 na spletnem naslovu http://www.mnz.gov.si/si/solidarnost_in_upravljanje_migracijskih_tokov/
36. Srića, V., Treven, S., & Pavlič, M. (1995). *Informacijski sistemi*. Ljubljana: Gospodarski vestnik.
37. *Širitev Schengenskega območja*. (2008). Časovni pregled. Najdeno 10. januarja 2009 na spletnem naslovu <http://www.ukom.gov.si/slo/koledar/dogodki/vstop-slovenije-schengen/schengen-casovni-pregled.pdf>
38. *THC-ePassports*. Najdeno 19. marca 2009 na spletnem naslovu <http://freeworld.thc.org/thc-epassport/>
39. *The Future of Biometrics (2009)*. Najdeno 10. januarja 2009 na spletnem naslovu <http://www.acuity-mi.com/hdfsjosg/euyotjtub/execsumm.pdf?code=S01>

40. *Uradni list L 239*. (2000a). Uradni list Evropske Unije L 239. Najdeno 10. januarja 2009 na spletnem naslovu [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922\(01\):SL:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(01):SL:HTML)
41. *Uradni list L 239*. (2000b). Uradni list Evropske Unije L 239. Najdeno 10. januarja 2009 na spletnem naslovu [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922\(02\):SL:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):SL:HTML)
42. *UREDBA SVETA o migraciji s schengenskega informacijskega sistema (SIS I+) na drugo generacijo schengenskega informacijskega sistema (SIS II)*. Najdeno 07. februarja 2009 na spletnem naslovu <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0197:FIN:SL:PDF>
43. *Uvajanje schengenskega režima*. Najdeno 31. januarja 2009 na spletnem naslovu <http://www.rtvlo.si/zgodbe/evropska-unija/uvajanje-schengenskega-rezima/14/arhiv>
44. *V Sloveniji smo začeli izdajati biometrične potne liste*. Najdeno 25. februarja 2009 na spletnem naslovu <http://www.mnz.gov.si/nc/si/splosno/cns/novica/article/12027/4795/>
45. Vintar, M. (1996). *Informatika*. Ljubljana: Paco.
46. *Za čim krajšo zamudo pri schengenu*. Najdeno 20. januarja 2009 na spletnem naslovu <http://www.delo.si/clanek/o160479>
47. Zetter, K. (2006, 03. avgust). *Hackers Clone E-Passports*. Najdeno 25. februarja 2009 na spletnem naslovu <http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=all>
48. Zetter, K. (2007, 01. avgust). *Scan This Guy's E-Passport and Watch Your System Crash*. Najdeno 25. januarja 2009 na spletnem naslovu <http://www.wired.com/politics/security/news/2007/08/epassport>
49. Zinrajh, Z. *Priprave Republike Slovenije na vstop v schengensko območje*. Najdeno 15. januarja 2009 na spletnem naslovu <http://www.planetgv.si/upload/htmlarea/files/5.%20dnevi%20evropskega%20prava/ZvonkoZinrajh.doc>