
UNIVERZITET SINGIDUNUM



DEPARTMAN POSTDIPLOMSKIH STUDIJA

MASTER RAD

ELEKTRONSKA IDENTIFIKACIONA DOKUMENTA NA BAZI SMART KARTICA

Mentor:
Prof. dr Mladen Veinović

Student: Branko Graovac
Br. indeksa: 55/2007

UNIVERZITET SINGIDUNUM



DEPARTMAN POSTDIPLOMSKIH STUDIJA

MASTER RAD

**MASTER STUDIJSKI PROGRAM:
Napredne informaciono komunikacione tehnologije**

TEMA:

**ELEKTRONSKA IDENTIFIKACIONA DOKUMENTA
NA BAZI SMART KARTICA**

Mentor:
Prof. dr Mladen Veinović

Student: Branko Graovac
Br. indeksa: 55/2007

ELEKTRONSKA IDENTIFIKACIONA DOKUMENTA NA BAZI SMART KARTICA

ELECTRONICALLY IDENTIFICATION DOCUMENTS On the basis of SMART CARD

Sažetak:

U ovom radu su izložene osnove koncepta elektronskog identifikacionog dokumenta, zasnovanog na tehnologiji SMART kartica, koji uz minimum preduslova omogućava izdavanje sigurnog i pouzdanog dokumenta za identifikaciju, kako u stvarnom tako i u digitalnom svetu. SMART kartica sa biometrijskim podacima vlasnika i infrastrukturu javnih ključeva, kao efikasnom zaštitom podataka na kartici i u elektronskim transakcijama (obezbeđuje pouzdanu proveru identiteta, poverljivost, integritet i raspoloživost podataka), predstavlja najsavremenije rešenje za identifikacioni dokument i znatno će doprineti efikasnosti državne administracije i smanjenju zloupotreba.

Informacione tehnologije su postale sastavni deo života svih nas. Elektronski podaci predstavljaju osnov za poslovanje preduzeća, ali i svakodnevni život fizičkih lica. Jedan od najsigurnijih načina hardverske zaštite podataka se zasniva na primeni tehnologije „pametnih“ kartica. U ovom radu su prikazani najčešći sistemi napada na „pametne“ kartice, kao i moguće metode zaštite njihovih podataka.

Dobro je poznato da su određene osobine ljudskog tela, kao što su DNK, otisak prsta i sl., karakteristične za svaku osobu, Sama biometrija predstavlja upotrebu bioloških karakteristika (lice, dužica oka, otisak prsta) ili osobina kao što su glas ili potpis sa ciljem potvrde identiteta osobe. Isto tako, predstavlja zamenu i daleko sigurniju varijantu zaštite od sistema zaštite zasnovanih na lozinkama.

U ovom radu izložene su osnove biometrijskih metoda, kao i način i pogodnosti njihove primene u sistemu MUP-a Republike Srbije za automatsku identifikaciju i verifikaciju građana

U ovom radu su izložene smernice i tehnološka pitanja, koja se razmatraju prilikom implementacije zaštićenih personalnih identifikacionih kartica. Razmatraćemo različite tehnologije koje danas postoje, s naglaskom na ulogu smart kartica u primeni sertifikovanih ličnih dokumenata. Ovaj rad opisuje i kako kombinacija smart kartica i biometrijskih tehnologija unapređuje sigurnost, tajnost i performense zaštićenih ID sistema.

Ključne reči:

PAMETNA kartica, identifikacioni dokument, Informacione tehnologije, biometrija, verifikacija

Abstract:

This document presents basic concept of electronic identity document based on SMART card technology, which provide minimum requirements for issuing secure and reliable document for identification, not only in physical world, but also in digital world. Combination of SMART card, biometrics and Public Key Infrastructure (PKI) as effective protection of data on the card and in electronical transactions (enable secure authentication, data confidentiality, data integrity and data availability), is most advanced solution for identification and will contribute appreciably to efficiency of government administration and reduction of identity frauds.

The information technologies time has already been developed and became an integral part of our lives. Electronic data is corresponding the principle of corporation trading, as also for physical persons everyday life. One of the most reliable aspects of hardware data protection is based on „smart“ cards usage technologies. In this paper we present the most prevailing data attacking systems as also possible data protection methods.

It is well known that determine characteristics of the human body are unique for the every person, just as is the DNA, fingerprint etc. Biometrics present the usage of physiological (the face image, iris, fingerprint...) and/or behavioral characteristic just as is the voice or the signature with the aim to confirms the identity of individual. Likewise, presents replacement and more secure kind of protection unlike the system with protection based on passwords.

This paper presents basic description of biometrics methods, as well as their benefits and applicability in the system for automatic identification and verification of citizens that will be deployed at the Ministry of Interior of the Republic of Serbia

This paper describes policy and technology issues that need to be considered in implementing secure personal ID cards. The different ID technologies that are available are considered, and the role that smart cards play in implementing certified personal credentials is presented. The paper describes how the combination of smart cards and biometric technologies enhances the security, privacy, and performance of secure ID systems.

Key words:

Smart card, Identification document, The information technologies, Biometrics, Verification

SADRŽAJ:

GLAVA I

1	UVOD.....	- 1 -
1.1	METODE ISTRAŽIVANJA.....	- 2 -
1.1.1	Ciljevi rada	- 2 -
1.1.2	Metodologija rada.....	- 2 -
1.2	TEHNOLOGIJA SMART KARTICA	- 3 -
1.3	STANDARDI.....	- 4 -
1.4	VRSTE KARTICA.....	- 5 -
1.5	VRSTE ČIP KARTICA.....	- 6 -
1.6	TIPOVI INFORMACIJA.....	- 9 -
1.6.1	TEHNOLOGIJE UPISA INFORMACIJA NA KARTICE	- 9 -
1.7	SMART KARTICE - ČITAČI I KOMUNIKACIJA	- 10 -
1.8	ULOGA SMART KARTICA U ZAŠTIĆENIM ID SISTEMIMA	- 12 -
1.8.1	PRIMENA SMART KARTICA.....	- 14 -
1.9	ZAKLJUČAK	- 15 -

GLAVA II

2	ZAŠTITA PODATAKA NA PAMETNIM KARTICAMA	- 16 -
2.1	UVOD.....	- 16 -
2.2	NAJČEŠI NAPADI NA PAMETNE KARTICE.....	- 17 -
2.3	MEHANIZMI ZAŠTITE PODATAKA NA ČIP KARTICAMA	- 21 -
2.4	ZAŠTITNA ULOGA SMART KARTICE.....	- 23 -
2.5	SIMETRIČNE I ASIMETRIČNE ENKRIPCije	- 24 -
2.5.1	Put do sigurnih podataka.....	- 24 -
2.5.2	Simetrično... ..	- 25 -
2.5.3	...ili asimetrično	- 26 -
2.5.4	Imenik kome (ne) verujemo	- 27 -
2.6	IDENTIFIKACIJA PUTEM RADIO FREKVENCije	- 28 -
2.6.1	Zaštita privatnosti i bezbednost podataka	- 28 -
2.6.2	Pitanje poverljivosti	- 29 -
2.6.3	Praćenje putnika putem pasoša koji nose.....	- 29 -
2.6.4	Teorija zavere	- 29 -
2.7	RFID metode zaštite	- 31 -
2.7.1	Faradejevi kavezi	- 31 -
2.7.2	Naredba KILL	- 31 -
2.7.3	Naredba SLEEP.....	- 32 -
2.7.4	Deljivi tagovi („Clip Tags“).....	- 32 -
2.8	Mogući napadi.....	- 33 -
2.9	ZAKLJUČAK	- 34 -

GLAVA III

3	BIOMETRIJSKE METODE U AUTOMATSKIM SISTEMIMA ZA IDENTIFIKACIJU I VERIFIKACIJU OSOBA	- 35 -
3.1	UVOD	- 35 -
3.2	BIOMETRIJSKI STANDARDI I METODE	- 36 -
3.3	BIOMETRIJSKE METODE.....	- 38 -
3.4	METODE PREPOZNAVANJA NA OSNOVU FIZIOLOŠKIH OSOBINA	- 39 -
3.4.1	Metoda prepoznavanja pomoću otisaka prstiju	- 39 -
3.4.2	Prepoznavanje na osnovu analize lica.....	- 40 -
3.4.3	Prepoznavanje na osnovu analize dužice oka.....	- 42 -
3.4.4	Identifikacija na osnovu senke	- 42 -
3.5	OBLASTI PRIMENE BIOMETRIJSKIH METODA	- 44 -
3.6	BIOMETRIKA I SMART KARTICE.....	- 45 -
3.7	ZAKLJUČAK	- 47 -
3.7.1	Da li nam je biometrika potrebna?.....	- 47 -

GLAVA IV

4	ELEKTRONSKI IDENTITET GRAĐANA I MOGUĆNOSTI NJEGOVE PRIMENE - 49 -	
4.1	UVOD	- 49 -
4.2	ELEKTRONSKI IDENTITET LIČNOSTI	- 50 -
4.3	ELEKTRONSKI IDENTIFIKACIONI DOKUMENTI.....	- 52 -
4.4	Elektronski identifikacioni dokumenti u Srbiji	- 54 -
4.4.1	Primena	- 54 -
4.5	Servis elektronske vlade (<i>e-vlada</i>)	- 58 -
4.6	Primena u zdravstvenoj zaštiti i osiguranju	- 59 -
4.7	MEĐUNARODNI ZAHTEVI, PREPORUKE I STANDARDI	- 60 -
4.8	DOMAĆI PROPISI	- 62 -
4.9	STANDARDIZACIJA	- 65 -
4.10	ZAKLJUČAK	- 66 -

GLAVA V

5	IDENTIFIKACIONI DOKUMENTI.....	- 67 -
5.1	UVOD	- 67 -
5.2	IDENTIFIKACIONI DOKUMENTI KOD NAS	- 68 -
5.3	KARAKTERISTIKE DOKUMENATA	- 68 -
5.3.1	Istina ili	- 69 -
5.3.2	Proizvodnja lične karte.....	- 70 -
5.4	Lična karta.....	- 72 -
5.4.1	Biometrija i dokumenta.....	- 73 -
5.4.2	Skeniranje bioloških osobina.....	- 74 -
5.4.3	Personalizacija	- 74 -
5.4.4	Personalizacija dokumenata	- 75 -
5.4.5	Zašto čip?	- 75 -

5.4.6	Korist od novih dokumenata	- 76 -
5.4.7	Distribucija dokumenata	- 77 -
5.5	Postupak izdavanja identifikacionog dokumenta.....	- 78 -
5.6	Izdavanje elektronskog identifikacionog dokumenta.....	- 80 -
5.7	KORIŠĆENJE eID	- 80 -
5.7.1	Iskustva drugih zemalja	- 81 -
5.7.2	Biometrijska dokumenta u regionu.....	- 82 -
5.8	DIGITALNI POTPIS	- 83 -
5.9	DIGITALNI SERTIFIKAT	- 85 -
5.9.1	Interna struktura.....	- 86 -
5.9.2	Put do sertifikata	- 86 -
5.9.3	Sertifikaciona tela	- 87 -
5.9.4	Globalna scena.....	- 87 -
5.10	eID I KVALIFIKOVANI SERTIFIKATI	- 88 -
5.11	Elektronski potpis i lična karta.....	- 89 -
5.11.1	Nije komplikovano	- 90 -
5.11.2	Potpis mnogo košta.....	- 90 -
5.12	Novi srpski pasoš - novo lice Srbije	- 91 -
5.12.1	Kako je počelo	- 91 -
5.12.2	Novi pasoši	- 92 -
5.13	Novi srpski pasoš crven i sa sedam nivoa zaštite.....	- 95 -
5.13.1	Šta je u čipu	- 96 -
5.13.2	Nije samo pasoš nezgodan	- 97 -
5.13.3	Bezbednije i brže na granicama	- 98 -
5.14	Identitet u par kilobajta	- 99 -
5.14.1	Prikupljanje podatka	- 99 -
5.14.2	Otisci prstiju	- 100 -
5.14.3	Softver	- 100 -
5.15	Čitač elektronske lične karte „ČELIK“	- 101 -
5.16	Testiranje putnih isprava (pasoši prolaze kroz „torturu“).....	- 102 -
5.17	MUP-u „Zlatni globus“ za uvođenje digitalnih dokumenata.....	- 104 -
5.18	ZAKLJUČAK	- 105 -
6	Literatura:	- 106 -

SPISAK SLIKA:

Slika 1 Vrste danas najčešće upotrebljivanih kartica.....	- 5 -
Slika 2 Šematski prikaz magnetne kartice.....	- 5 -
Slika 3 Vrste "čip" kartica koje su danas u upotrebi.....	- 6 -
Slika 4 Izgled čip kartice sa dodatkom magnetnog zapisa	- 6 -
Slika 5 Šematski prikaz preseka čip kartice	- 8 -
Slika 6 Izgled tipičnog modula	- 8 -
Slika 7 Čitač smart kartice	- 10 -
Slika 8 Kartice sa direktnim fizičkim kontaktom	- 11 -
Slika 9 Kartice bez direktne veze sa čitačem	- 11 -
Slika 10 Mogući napadi na čip karticu po nivoima.....	- 17 -
Slika 11 Klasifikacija mogućih tipova napadača	- 17 -
Slika 12 Broj kombinacija šifre vezan za dužinu kjuča	- 19 -
Slika 13 Kombinacije koje napadač mora da „isproba“ u zavisnosti od dužine šifre (za 26 karaktera)	- 19 -
Slika 14 Br. kombinacija ako su korišćena i velika i mala slova i brojevi bez znakova.	- 20 -
Slika 15 Osnovne komponente sigurnosti smart kartice	- 21 -
Slika 16 Primer asimetrične kriptografije	- 24 -
Slika 17 Upisivanje korisnika u biometrijski sistem.....	- 36 -
Slika 18 Verifikacija / identifikacija na osnovu biometrijskih podataka	- 37 -
Slika 19 Otisak prsta i minucije	- 39 -
Slika 20 Prilagodljivost sistema kod LFA metode.....	- 41 -
Slika 21 LFA metoda.....	- 41 -
Slika 22 Struktura oka.....	- 42 -
Slika 23 Identifikacija na osnovu senke	- 43 -
Slika 24 Zastupljenost biometrijskih metoda na tržištu	- 44 -
Slika 25 Skeniranje dokumenata osvetljenog različitim vrstama svetlosti	- 55 -
Slika 26 Prikaz dekodiranih podataka iz 2D barcoda.....	- 55 -
Slika 27 Zapis MRZ iščitao OCR-B-om.....	- 55 -
Slika 28 Uzimanje alive otiska prsta i njegovo poređenje sa zapisom na dokumentu ...	- 55 -
Slika 29 Primena u okviru e-Police	- 56 -
Slika 30 Radna stanica za kontrolu prelaska državne granice	- 56 -
Slika 31 Fizička kontrola pristupa zaštićenim oblastima	- 57 -
Slika 32 Nova LK u čitaču.....	- 69 -
Slika 33 Pametna kartica	- 70 -
Slika 34 Prednja strana nove LK.....	- 72 -
Slika 35 Druga strana LK bez čipa	- 72 -
Slika 36 Blanko obrazac - prednja strana	- 72 -
Slika 37 Blanko obrazac sa čipom - druga strana.....	- 72 -
Slika 38 Nova biometrijska LK.....	- 73 -
Slika 39 Stara LK.....	- 73 -
Slika 40 Tabla za potpis.....	- 74 -
Slika 41 Skener za otisak prsta	- 74 -
Slika 42 Proizvodna traka LK	- 78 -
Slika 43 Pakovanje LK.....	- 78 -
Slika 44 Digitalno potpisivanje	- 83 -
Slika 45 Identifikacija digitalnim potpisom	- 84 -
Slika 46 Primer sertifikata	- 85 -
Slika 47 Blanko obrazac	- 89 -

Slika 48 Novi pasoš.....	- 91 -
Slika 49 Druga strana pasoša	- 93 -
Slika 50 Unutrašnje stranice novog srpskog pasoša	- 93 -
Slika 51 Princip novih biometrijskih pasoša.....	- 94 -
Slika 52 Proizvodna traka za nove pasoše.....	- 94 -
Slika 53 Primer čipa sa antenom.....	- 96 -
Slika 54 Detalj iz proizvodnje ličnih karti u Zavodu za izradu novčanica u Beogradu .	- 99 -
Slika 55 Način očitavanja čipa elektronske lične karte	- 101 -
Slika 56 Aplikacija ČELIK.....	- 101 -
Slika 57 Detalj sa proizvodne trake.....	- 102 -
Slika 58 Testiranje neprekidnim pisanjem	- 103 -
Slika 59 Neprekidno otvaranje i zatvaranje.....	- 103 -
Slika 60 Tri hiljade udaraca po pasošu	- 103 -
Slika 61 Detalj sa ceremonije	- 104 -

SPISAK TABELA:

Tabela 1 . Zahtevane memorijski prostor za različite biometrike	- 9 -
Tabela 2 Standardne dužine ključa.....	- 18 -
Tabela 3 Potrebno vreme za otkrivanje šifre.....	- 18 -
Tabela 4 Vreme potrebno za otkrivanje šifre na osnovu njene ukupne dužine i korišćenih karaktera (mala i velika slova i brojevi, bez specijalnih karaktera)	- 20 -

SKRAĆENICE

AFIS - Automatic Fingerprint Identification System
BAC - Basic Access Control
BioAPI - Biometric Application Program Interface
CA - Certificate Authority
CBEFF - Common Biometric Exchange File Format
COS - Card Operating System
CRL - Certificate Revocation List
CV - Country Verifiable
DES - Data Encryption Standard
ECC - Elliptic Curve Cryptography
eID - Elektronski identifikacioni dokument
EPROM - Erasable Programmable Read Only Memory
EEPROM - Electrically EPROM
FAR - False Accept Rate
FRR - False Reject Rate
HSM - Hardware Security Module
IAS - Identification, Autentication & Signature
ICAO - International Civil Aviation Organization
ISO - International Standards Organization
ISO/IEC - Međunarodna organizacija za standardizaciju i Međunarodna elektrotehnička komisija
ITSEC - Information Technology Security Evaluation Criteria
JMBG - jedinstveni matični broj građana
JTC-1 - Joint Committee 1
LDS - Logical Data Structure
MRZ - Machine Readable Zone
OCR - Optical Character Recognition
OCSP - Online Certificate Status Protocol
PKI - Public Key Infrastructure
RA - Registration Authority
RFID - Radio Frequency Identification
RSA - Rivest, Shamir, and Adleman
SSCD - Secure Signature Creation Device
WORM - Write Once Read Many
WSQ - Wavelet Scalar Quantization
ZIN - Zavodu za izdavanje novčanica

GLAVA I

1 UVOD

Visoka tehnologija i sigurnost karakteristika su današnjih pametnih kartica. U današnjem svetu u kojem tehnologija uzima sve više maha i nastaju mnoge nove usluge s ciljem da nam na razne načine olakšaju život, a ključna reč je konvergencija. Ona znači objedinjavanje više različitih usluga pa čak i uređaja u jedan.

Identifikacija podrazumeva korišćenje nekog znaka (*token*), koji sadrži podatke o entitetu. Token može biti barkod, slika, i/ili dijagram, na papiru, plastici, nalepnici ili čipu. Podaci se mogu podeliti na podatke koji služe za potvrdu identiteta, podatke koji predstavljaju spisak ovlašćenja i rokove važenja tih ovlašćenja, kao i podatke koji opisuju funkcije koje osoba obavlja. Token mora biti personalizovan: postoji jednoznačna veza između entiteta i znaka (*npr. fotografija ili otisak prsta*).

Poslednjih godina pojavila se potreba za pouzdanim i brzim identifikovanjem populacije, i kao odgovor na ovaj problem informatičke kompanije širom sveta su počele da razvijaju sisteme za masovnu produkciju visoko zaštićenih identifikacionih dokumenata građana. Identifikaciona dokumenta u obliku kartica mogu se koristiti za sledeće namene:

- nacionalne ID kartice građana
- višenamenske nacionalne ID kartice građana
- pasoši
- studentske ID kartice i ID kartice za zaposlene
- višenamenske studentske i ID kartice za zaposlene
- dozvole (*vozačke, za nošenje oružja, itd.*)
- propusice (*za posao, posetioce, parking, za životinje, itd.*)
- ID kartice za zdravstveno osiguranje
- ID kartice za socijalnu zaštitu, socijalnu pomoć i penzije
- članske kartice
- ID kartice za životinje
- kartice za kupovinu određenih proizvoda
- kartice za zaštitu uređaja i terminala
- kartice za biometrijski pristup
- ostalo

Nova, napredna tehnologija sigurno može da pomogne u uspostavljanju jednog pouzdanog sistema identifikacije lica i zaštite identifikacionih dokumenata koji će, na prvom mestu, povećati njihovu upotrebljivost i pouzdanost, te dalje doprineti smanjenju zloupotreba. SMART kartica sa biometrijskim podacima vlasnika¹ i infrastrukturom javnih ključeva - PKI², koja štiti podatke u čipu kartice i elektronskim transakcijama (*omogućava pouzdanu autentikaciju, tajnost, integritet i raspoloživost podataka*), nameću se kao prirodno rešenje za pouzdan identifikacioni dokument kako u realnom tako i u svetu digitalne komunikacije.

¹ digitalna fotografija obavezno i opciono otisak prsta, analiza dužice oka ili DNK analiza

² PKI - Public Key Infrastructure

1.1 METODE ISTRAŽIVANJA

1.1.1 Ciljevi rada

Ovaj rad ima prevashodni cilj da nas upozna sa elektronskim identifikacionim dokumentima, smart karticama, njihovom standardu, tehnologiji i primeni, naravno i sigurnosti.

Pored toga rad treba da ukaže na prednosti korišćenja elektronskih identifikacionih dokumenata i da ukaže na širok spektar mogućnosti koje se nude krajnjim korisnicima.

1.1.2 Metodologija rada

„Najjednostavnija je definicija „**metodologije**“ (grčki „*metodhs* + *logos*“ = *reč, govor, nauka o metodama naučnog istraživanja*) da je to nauka o metodama naučnog istraživanja. U širem smislu metodologija je nauka o celokupnosti svih oblika i načina istraživanja pomoću kojih se dolazi do sistemskog i objektivnog naučnog znanja, ili naučna disciplina u kojoj se kritički ispituju i eksplicitno izlažu različite opšte i posebne naučne metode, naziva se metodologija “.³

U ovom radu, da bi se postigli postavljeni ciljevi kao i što efikasniji rezultat koji se dobijaju povezivanjem i odgovarajućom kombinacijom više naučnih metoda, korištene su sledeće metode:

- metoda deskripcije,
- komparativna metoda,
- matematička metoda,
- metoda analize,
- metoda sinteze

Metoda deskripcije, definisana kao postupak jednostavnog opisivanja ili ocrtavanja činjenica, procesa i predmeta, te njihovih empiriskih potvrđivanja odnosa i veza, ali bez naučnog tumačenja i objašnjavanja, je korišćena kroz celi rad.

Komparativna metoda, koja podrazumeva upoređivanje istih ili srodnih činjenica, pojava, procesa i odnosa, odnosno utvrđivanje njihove sličnosti u ponašanju i intenzitetu kao i razlika među njima.

Matematička metoda, je naučni sistemski postupak, a sastoji se u primeni matematičke logike, simbola, brojnih matematičkih operacija. Kratko rečeno predstavlja matematički način zaključivanja.

Metoda analize, je postupak naučnog istraživanja i objašnjavanja stvarnosti putem raščlanjivanja složenih misaonih tvorevina (*pojmovi, sudovi i zaključci*) na njihove jednostavnije delove i elemente, kao i izračunavanje svakog dela (*elementa*) za sebe i u odnosu na druge delove, celine.

Metoda sinteze, je suprotna metoda od analize koja se takođe primjenjivala u izradi ovog rada.

³ Prof.dr.Čekić Š.: „Osnovi metodologije i tehnologije izrade znanstvenog i stručnog djela“, Sarajevo 1999., str.33

1.2 TEHNOLOGIJA SMART KARTICA

SMART kartica je plastična kartica pravougaonog oblika sa ugrađenim elektronskim kolom (*čipom*), koji u funkcionalnom smislu predstavlja miniračunar sa mikroprocesorom i memorijom za čuvanje i obradu podataka, smeštenim ka središnjem levom delu kartice.

Podela dokumenata zasnovanih na SMART karticama:

1. Po dimenzijama:

- **ID1 format** (54,0mm X 85,6mm, debljine 0,25 - 1,25mm) je najčešće korišćen za identifikaciona dokumenta, zdravstvene kartice, vozačke dozvole, saobraćajne dozvole, kartice za zaposlene, vojne legitimacije...
- **ID2 format** (74,0mm X 105,0mm, debljine 0,25 - 1,25mm) je manje zastupljen format za identifikaciona dokumenta kao i format sadašnjih viza koje se pripajaju putnoj ispravi;
- **ID3 format** je format sadašnjih i budućih elektronskih putnih isprava čija se primena počela tokom 2004/2005.

Očitavanje podataka se vrši istim čitačem, jer je položaj mašinski čitljivih zona na različitim formatima isti.

2. Po vrsti integrisanog kola razlikujemo:

- Dokumenta sa memorijskim čipom koji služi samo za čuvanje podataka. Mogu biti:
 - sa EPROM⁴ čipom, kod kojih se memorija menja samo jednom, ili
 - sa EEPROM⁵ čipom, kod kojih se memorija može menjati do 100.000 puta.
- Dokumenta sa mikroprocesorskim čipom sa memorijom koji osim čuvanja podataka omogućava i njihovu obradu, slično mini računaru. Čip ovakvog dokumenta sadrži CPU za obradu podataka i koprocesore za realizaciju zaštitnih funkcija, RAM za privremene kalkulacije i ROM za memorisanje programa i operativnih instrukcija.

3. Prema načinu komunikacije između dokumenta i čitača kartica, razlikujemo:

- **Dokument sa direktnim očitavanjem podataka**, sa kontaktnim čipom kod koga se očitavanje podataka vrši stavljanjem dokumenta u čitač. Najčešće se primenjuje kod dokumenata sa memorijskim i mikroprocesorskim čipovima, ID1 i ID2 formata.
- **Dokument sa indirektnim očitavanjem podataka** sa beskontaktnim čipom kod koga se komunikacija obavlja indirektnim putem (*preko ugrađene radio antene dometa do 10 cm ili putem elektromagnetnih talasa*). Najčešće se primenjuje za dokumente ID3 formata, odnosno, putnu ispravu.
- **Dokument sa kombinovanim očitavanjem podataka** kod koga se očitavanje podatka može vršiti direktnim kontaktom i radio vezom sa čitačem.

⁴ EPROM - Erasable Programmable Read Only Memory

⁵ EEPROM - Electrically EPROM

1.3 STANDARDI

U identifikacionim sistemima se koriste različite tehnologije. Šarolikost u tehnologijama otežava otkrivanje falsifikata, ograničava korišćenje i mogućnost širenja kartica i često sužava izbor proizvođača.

Idealan sistem definiše jednu otvorenu arhitekturu za kartice i za dodatnu opremu, korišćenjem standarda za specifikaciju kartica. Ti standardi omogućavaju da se kartice koriste za različite servise i dozvoljavaju organizacijama da naručuju kartice od različitih proizvođača, pa samim tim zbog veće konkurencije i cene postaju niže.

Osnovni standard za kontakt smart kartice je ISO⁶ 7816 koji ima deset delova, a za smart kartice sa radio-frekvencijskim očitavanjem standard je ISO 14443. Ovi standardi određuju fizičke, električne i mehaničke karakteristike, kao i aplikativni interfejs.

Standard za mašinski čitljive putne isprave (*pasoš, vize itd.*) je ICAO⁷ 9303. Ovaj dokument integrisan je sa ISO standardom 7501 (*7501-1, 7501-2 i 7501-2*) i propisuje minimum zahteva koje putne isprave treba da zadovolje da bi bile mašinski čitljive.

Dokument Evropske zajednice takođe propisuje minimalne zaštitne standarde za putne isprave za zemlje članice (*pasoši, službeni pasoši, diplomatski pasoši, propusnice za putovanja i identifikacione kartice*). Prema ovim dokumentima materijal mora da podnosi određeni stepen deformacija koje su prisutne u normalnim uslovima (*npr. uvrtanje*), ne sme da bude toksičan, mora biti otporan na hemikalije sa kojima može doći u dodir u toku uobičajne upotrebe, mora biti termički stabilan, otporan na vlažnost, mašinski čitljiv pri vazdušnoj vlažnosti od 5 do 95%, ne sme da bude autorefleksivan, mora da ima na svakoj strani vođeni žig u dve nijanse, i opcione elemente zaštite.

Ovaj dokument razmatra i sigurnosne aspekte: mašinski čitljive putne isprave moraju biti osigurane od falsifikovanja, promena podataka na kartici, pokušaja lažnog predstavljanja.

Materijal mora da bude zaštićen dodatnim sigurnosnim mehanizmima, kao što su sigurnosne niti i vlakna u boji. Tehnike štampe koje se koriste su: offset štampa pozadine, sa UV-fluorescentnom štampom i mikroštamptom, dok se prilikom personalizacije koriste laserska štampa, termo-transfer, fotografska štampa, štampa u boji, lasersko graviranje i digitalna ofset štampa. Definisane su tri dimenzije kartica: ID-1, ID-2 i ID-3, koje se sve mogu očitavati jednim čitačem jer je položaj mašinski čitljivih zona isti. Kartica je podeljena u sedam zona od I do VII. Zone I-VI se mogu vizuelno pregledati. Zona VII se može čitati samo mašinski.

⁶ ISO - International Standards Organization

⁷ ICAO - International Civil Aviation Organization

1.4 VRSTE KARTICA

Pametna kartica je najmlađi član porodice identifikacionih kartica. Zbog potrebe da se sa postojećih sistema identifikacije (*magnetne kartice i reljefne kartice*) ostvari prelaz na novu tehnologiju koja podrazumeva kartice sa čipom u sebi, one još uvek objedinjavaju sve ove stare karakteristike. Bez obzira što pametna kartica još sadrži na sebi i magnetnu traku ili reljefne podatke, njena osnovna karakteristika je čip.

Postoji veliki broj različitih kartica koje se danas koriste, ali se u osnovi dele u dve grupe (*aktivne kartice i pasivne kartice*) kao što je to prikazano na slici 1.



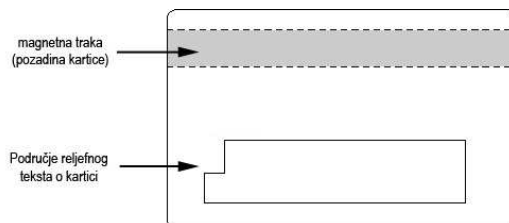
Slika 1 Vrste danas najčešće upotrebljivanih kartica

Osnovna razlika između pasivnih i aktivnih kartica je u tome što pasivne kartice nemaju mogućnost za bilo kakvom interakcijom sa čitačem. Njihova osnovna funkcija je u jednokratnom ili višekratnom memorisanju nekog tipa informacije, bez mogućnosti da vrše bilo kakvo procesiranje. Procesiranje podataka koji su u kartici ili dolaze ka kartici od strane komunikacionog uređaja, je moguće samo ukoliko na kartici postoji čip koji to omogućava.

Reljefna kartica je potpuno zastareli tip kartica koji nema nikakvu mogućnost zaštite.

Magnetna kartica je uvedena u upotrebu u SAD-u 1970. godine, kada započinje njena masovna upotreba. Širom sveta se pojavljuju prodavnice koje primaju kartice, a broj korisnika se iz dana u dan povećavao.

Magnetni zapisi na plastičnim karticama su i dalje aktuelni, ali magnetne kartice polako izlaze iz upotrebe, tako što se umesto njih uvode čip kartice.



Slika 2 Šematski prikaz magnetne kartice

Za razliku od čip kartica, magnetne kartice na sebi nose izuzetno malu količinu informacija, bez mogućnosti ostvarenja visokog nivoa zaštite, kao i bez mogućnosti bilo kakve interakcije sa čitačem. Zbog drastičnog pada cene čipovima, magnetne kartice polako odlaze u zaborav, iako su godinama bile izuzetno korišćene.

1.5 VRSTE ČIP KARTICA

ČIP kartice se mogu razvrstati u dve osnovne grupe:

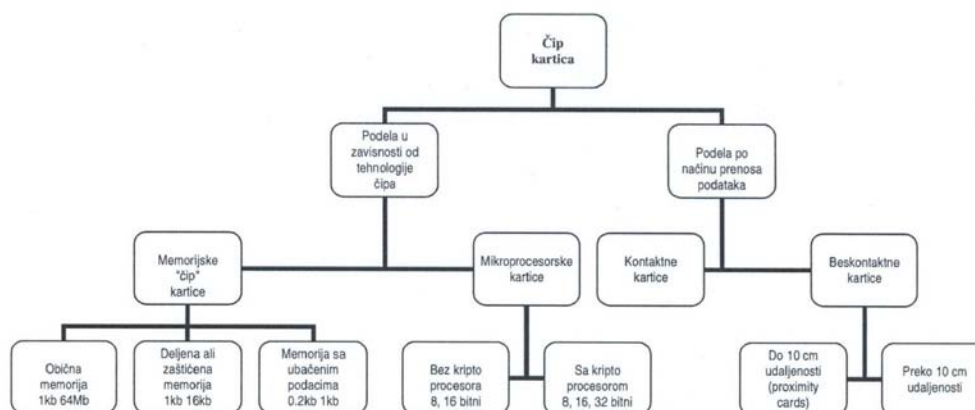
U zavisnosti od čipa, kartice delimo na:

- memorijske kartice (**a1**) i
- mikroprocesorske kartice (**a2**)

Po načinu prenosa podataka, kao i po načinu pristupa razlikujemo:

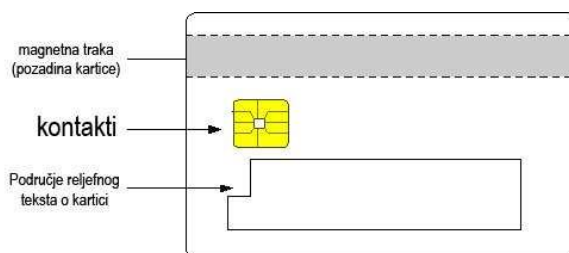
- kontaktne (**b1**),
- beskontaktne (**b2**) i
- kombinovane kartice (*imaju implementirane obe vrste prenosa podataka*).

Svaku od tih grupa možemo dalje deliti s obzirom na veličinu i tip memorije, kao i na osnovu prisutnosti procesora (*podela u zavisnosti od tehnologije čipa*). Procesor daje kartici pravu „pamet“. Memorijske kartice, ne spadaju u grupu pametnih kartica iako imaju čip na sebi, dok se često, greškom, naziv „pametna“ kartica koristi za sve kartice sa čipom. Naziv „pametna“ kartica se veže samo za mikroprocesorske kartice. Naziv „čip kartica“ obuhvata i memorijske i mikroprocesorske kartice.



Slika 3 Vrste "čip" kartica koje su danas u upotrebi

Klasifikacija kartica koje na sebi imaju čip je grafički prikazana na slici 3. Na osnovu ove slike je lako zaključiti koje kartice spadaju u „pametne“, a koje ne. Moguće su i kombinacije dve tehnologije na jednoj kartici, kao na primer: magnetna + čip kartica i slično.



Slika 4 Izgled čip kartice sa dodatkom magnetnog zapisa

Na slici 4 je šematski prikazan izgled kartice sa čipom u slučaju da se na njoj nalazi magentna traka ili samo područje za reljefni zapis podataka. Najčešće je na ovakvim karticama ostavljen prostor za reljefni zapis.

a1) Memorijska kartica ima ugrađen čip s memorijom i neprogramabilnom logikom, jer ne sadrži mikroprocesor. Usled neprisustva mikroprocesora, neprogramabilna logika obrađuje podatke. Ona omogućava direktan pristup memoriji i podržava nekoliko neprogramabilnih naredbi. Memorija kartice obično ima kapacitet od oko 4KB za podatke.

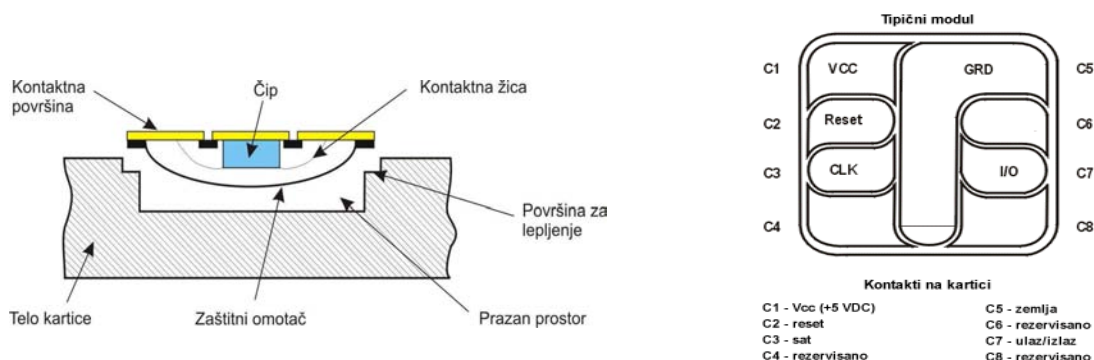
a2) Mikroprocesorska kartica je čip kartica koja u svom sastavu ima funkcionalan mikroprocesor. Mikroprocesor omogućava ugradnju kriptografskih algoritama i primenu širokog skupa zaštitnih mehanizama. Funkcionalnost mikroprocesorskih kartica ograničena je samo veličinom njihove memorije i mogućnostima ugrađenog procesora. Koriste se u aplikacijama koje zahtevaju sigurnost i privatnost podataka, kao što su:

- kontrola pristupa,
- bankarske aplikacije,
- aplikacije bežičnih telekomunikacionih sistema itd.

Ovakav tip kartica ima naziv „**pametne**“ kartice. One su sposobne za dinamičko obrađivanje podataka, pošto pored procesora, najčešće sadrže i ulazno - izlaznu jedinicu, kao i više vrsta memorija. Trenutno se upotrebljavaju 8-bitni, 16-bitni i 32-bitni procesori, sa u proseku 64 KB ROM-a, 16 do 32 KB EEPROM-a i 3 KB RAM-a. Ulazno - izlazna jedinica dostiže brzinu prenosa od 9,6 kbps -115 kbps.

Veliki broj današnjih mikroprocesorskih kartica ima krypto - koprocessor u sebi, zarad povećanja nivoa sigurnosti. One su sposobne za generisanje i proveravanje digitalnih potpisa, kao i za šifrovanje podataka sa simetričnim ključem. Podaci su organizovani po sistemu datoteka, a do njih procesor ima pristup uz pomoć operativnog sistema kartice COS⁸. Ovakve mikroprocesorske kartice se upotrebljavaju u telefonima GSM (*kartica SIM*), za autentikaciju, čuvanje poverljivih podataka (*na primer, privatnih ključeva, sertifikata itd.*).

b1) Kontaktne kartice komuniciraju sa čitačem kartica preko osmoportnog priključka. Ova površina preko koje se ostvaruje mehanička i električna veza sa čitačem je dimenziono i oblikom standardizovana. Kartica nema svoj izvor napajanja i nema mogućnost unutrašnje generacije signala takta.



⁸ COS - Card Operating System

Slika 5 Šematski prikaz preseka čip kartice

Slika 6 Izgled tipičnog modula

Čip je najvažniji element „pametne“ kartice. Za razliku od magnetne trake, čip je lomljiv i ne može se jednostavno nalepiti na površinu kartice. Umesto toga se čip stavlja u neku vrstu kućišta, tako da bude zaštićen od spoljašnjih uslova svakodnevnog korišćenja kartice. To kućište se naziva „modul čipa“. Struktura modula i proces postavljanja čipa u telo kartice prikazani su na slici 5.

Većina danas primenjivanih kartica se zasniva na kontaktu sa čitačem.

b2) Zbog toga što kontaktne kartice zahtevaju tačno definisani položaj i orijentaciju kartice prilikom stavljanja u uređaj za njeno čitanje, u situacijama gde su potrebne brze transakcije se upotrebljavaju beskontaktno kartice. Beskontaktno kartice za razliku od kontaktnih sa spoljašnjim svetom komuniciraju preko ugrađene antene. Ova antena se nalazi u telu kartice. Napajanje ovakve čip kartice se izvodi sa internom baterijom ili elektromagnetskom indukcijom kroz ugrađenu antenu. Podaci se do uređaja za čitanje prenose elektromagnetnim poljem. Visoko frekventno elektromagnetno polje ima dvostruku ulogu, a to su:

- uloga prenosa energije elektromagnetnom indukcijom
- uloga prenosa podataka faznom ili amplitudnom modulacijom.

Ovakve beskontaktno kartice (*proximity cards*) imaju svoje prednosti i mane. Prednosti beskontaktnih kartica su u tome što je čip u potpunosti integrisan u telo kartice i ne ostvaruje se mehanički kontakt sa čitačem. To znači da ne postoji mogućnost naponskog i strujnog udara i da nema trošenja kontaktnih površina učestalim korišćenjem kartice. Time se produžuje životni vek kartice. Otpornost beskontaktnih kartica i izdržljivost odgovarajućih uređaja za njihovo očitavanje čini takve sisteme idealnim za industrijska okruženja.

Nedostaci beskontaktnih kartica su malobrojni. Osnovna mana je obavezna maksimalna udaljenost u odnosu na čitač kartica (*udaljenost do 10cm*). Zbog mogućeg kratkog vremena transakcije prenosi se samo ograničena količina podataka. Povećana je osetljivost na mehaničko oštećenje ako dođe do savijanja i uvijanja plastične osnove kartice. Postoji i potencijalna opasnost da se bez znanja vlasnika kartice izvede novčana transakcija ili da se presretnu poslati podaci. Najvažniji nedostatak je visoka cena beskontaktnih kartica, što ne važi i za kontaktne. Standardi vezani za beskontaktno kartice su još uvek u fazi izrade, što predstavlja dodatni razlog za češće korišćenje kontaktnih kartica.

Osnova „pametne“ kartice je u svakom slučaju ista, tako da se dodatkom plastike oko centralnog dela (*ID-000*) može dobiti bilo koja od preostale dve. Razlika je samo u uređajima za koji su čip kartice namenjene, tako da i njihova veličina varira. Funkcije su u sva tri slučaja potpuno nepromenjene a veličine različite. Za mobilnu telefoniju (*SIM Cards*) se na primer koristi najmanji standard (*ID-000*), sa odgovarajućim kontaktima.

1.6 TIPOVI INFORMACIJA

Zaštićene ID kartice uključuju alfanumeričke informacije (*ime i prezime vlasnika, pol, datum rođenja, datum izdavanja, datum do kada kartica važi, serijski broj, mesto za potpis i drugo*), fotografiju, jednu ili više biometričkih informacija, kao i zaštitne funkcije (*digitlni potpis i javne/privatne ključeve*).

Biometrički podaci se smeštaju na karticu i onda verifikuju uzimanjem biometričkih podataka od osobe u tački interakcije. Pomoću pouzdanog snimanja i provere jedinstvenih biometričkih podataka osobe, kao što su otisak prsta, otisak dlana, analiza lica itd., sistem može da potvrdi identitet. U *Tabeli 1.* date su potrebne veličine memorijskog prostora za smeštanje različitih biometričkih podataka.

Smart kartice imaju veće memorijske kapacitete od drugih kartica, pa su daleko atraktivnije za sisteme koji koriste biometriku, kao dodatni zaštitni mehanizam (*uz PIN kod, sertifikat, digitalni potpis*).

Biometrika	Zahtevana memorija (Byte)
Skenirani otisak prsta	300 – 1200
Geometrija otiska prsta	14
Prepoznavanje dužice oka	512
Verifikacija glasa	1500
Prepoznavanje lica	500 – 1000
Verifikacija potpisa	500 – 1000
Prepoznavanje mrežnjače oka	96
.	.

Tabela 1 . Zahtevane memorijski prostor za različite biometrike

1.6.1 TEHNOLOGIJE UPISA INFORMACIJA NA KARTICE

Postoji više tehnologija za upisivanje informacija na kartice:

- termalna štampa,
- mikroštampa,
- embosiranje,
- indent štampa i
- tehnika laserskog graviranja.

Vidljivo odštampane identifikacione informacije (*ime osobe, adresa, fotografija itd.*) se vizuelno verifikuju prilikom identifikacije. Informacije, koje ne treba da budu vizuelno čitljive, skladište se na neki od sledećih načina:

- Bar kodovi
- Magnetne trake.
- Optičke trake.
- Integrisano kolo na smart karticama.

1.7 SMART KARTICE - ČITAČI I KOMUNIKACIJA

Čitač obezbeđuje vezu između kartice i sistema koji pruža neku uslugu (*servis*), tako što daje potrebno napajanje, inicijalizuje karticu i posreduje između kartice i sistema. Inicijalizacija kartice je određeni protokol koji svaka kartica mora da izvrši. Svaki čitač podržava inicijalizaciju bilo koje kartice, ali ne obavezno i aplikaciju koju kartica obavlja posle inicijalizacije. Uloga čitača zavisi od tipa kartice. Kod kartica sa memorijskim čipom čitač ima uvid u strukturu memorije i adresni prostor, i radi kao prevodilac u komunikaciji kartice i sistema - čitač je svestan kartice (*aware mode*). Kod kartica sa mikroprocesorskim čipom čitač je upoznat sa logičkom strukturom kartice, služi samo za prenošenje naredbi od sistema ka kartici, bez ikakvih izmena i to je generički pristup (*generic mode*).

Sa hardverskog stanovišta postoje dva tipa čitača: transparentni i samostalni. Transparentni čitači zahtevaju podršku računarskog sistema za sve funkcije, uključujući inicijalizaciju i samu aplikaciju (*sistem upravlja i čitačem i karticom*). Samostalni čitači, ili terminali, imaju svu logiku potrebnu za inicijalizaciju i posredovanje u komunikaciji kartice i sistema, bilo da se radi o aware ili generic mode-u.

Čitači smart kartica trenutno predstavljaju jedan od problema za uvođenje široke primene smart kartica - smart kartica je upotrebljiva samo ukoliko postoje i odgovarajući čitači, i to na svim mestima na kojima osoba zahteva neku uslugu ili dokazuje svoj identitet, a njih ima dosta (*državne institucije, domovi zdravlja i bolnice, studentski domovi itd.*).

U zavisnosti od vrste kartice koriste se različiti metodi i tehnike za očitavanje podataka, da bi se očitale informacije sa kartica neophodno ih je:

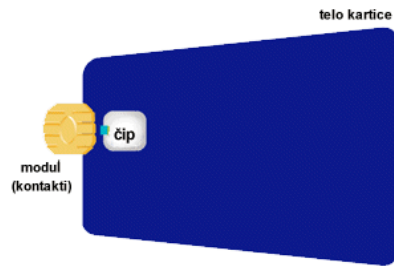
- provući kroz čitač (*read-only magnetne kartice*),
- skenirati (*kartice koje sadrže bar kodove*),
- očitati pomoću senzora (*smart kartice*) ili
- staviti u čitač (*kartice sa read/write magnetnom trakom, optičke ili smart kartice*).



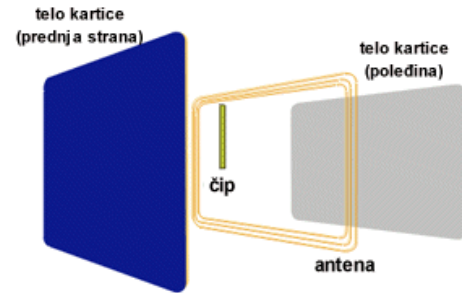
Slika 7 Čitač smart kartice

Čip smart kartice i čitač komuniciraju putem direktne fizičke veze ili putem radio signala, i u skladu s tim postoje kartice za direktni kontakt, kartice za komunikaciju putem radio signala i kombinovane kartice.

Čitači sa direktnim fizičkim kontaktom mogu da se koriste za kartice sa memorijskim čipom i za kartice sa mikroprocesorskim čipom, za obe veličine kartica. Na kartici postoji 8-pinski kontakt, *slika 6*, tj. mikromodul koji se fizički povezuje sa čitačem.



Slika 8 Kartice sa direktnim fizičkim kontaktom



Slika 9 Kartice bez direktne veze sa čitačem

Kartice kod kojih se uspostavlja radio veza sa čitačem izgledaju kao na slici 9.

Ovaj metod primenjuje se kod kartica sa memorijskim čipom, i to samo za kartice dimenzije kreditnih kartica. Antena ima domet oko 10cm i napaja se signalom generisanim sa čitača. Identifikacioni bedževi za zaposlene koje velike firme koriste za kontrolu ulaska u prostorije predstavljaju tipičan primer primene.

Kombinovane smart kartice su hibridna kombinacija dva prethodna metoda, imaju i 8-pinski kontakt za direktni čitač i antenu za radio komunikaciju sa čitačem.

1.8 ULOGA SMART KARTICA U ZAŠTIĆENIM ID SISTEMIMA

Smart kartice su široko prihvaćene kao najzaštićenija i najpouzdanija forma elektronske identifikacije, pa su, najčešće u upotrebi kao personalne ID kartice. Treba naglasiti da je opšta tendencija da se koriste za zaštitu promenljivih i najpoverljivijih podataka. One dozvoljavaju i online i offline pristup informacijama i servisima. Smart kartice mogu da skladište, štite i dozvoljavaju promene informacija smeštenih u mikročip na kartici. Mogućnost dinamičke komunikacije kartica i informacionih sistema ubrzava tradicionalno spor proces identifikacije, automatizuje operacije i smanjuje cenu korišćenja usluga. Smart kartice mogu da sadrže mnogostrukе aplikacije i da objedinjuju veći broj servisa. Danas je glavni trend razdvajanje operativnog sistema koji koristi čip smart kartice i aplikativnog softvera i njihova standardizacija. Ovo će omogućiti primenu raznorodnih aplikacija za najrazličitije usluge i potrebe pomoću samo jedne smart kartice. Dodatno, ide se ka tome da se korisniku omogući da postojećoj smart kartici dodaje nove aplikacije i funkcije.

Fizički i digitalni identitet. Smart kartice obezbeđuju jedinstvenu mogućnost kombinovanja identifikacije i verifikacije i u fizičkom, stvarnom i u digitalnom svetu.

Zaštićena fizička identifikacija obezbeđena je preko vidljivo odštampanih informacija i zaštitnih štamparskih tehnologija.

Fizička verifikacija postiže se korišćenjem jedinstvenog PIN koda za karticu ili smeštanjem jedinstvenih biometričkih informacija vlasnika kartice na čip. Oba ova prilaza dozvoljavaju korišćenje smart kartica tek pošto se vlasnik kartice uspešno verifikuje pomoću podataka smeštenih na čipu.

Digitalna identifikacija omogućena je preko ličnih informacija smeštenih na čipu a koje se odnose na identifikaciju ili funkciju koju osoba treba da potvrdi u određenoj transakciji.

Digitalna verifikacija obezbeđena je preko kriptografskih ključeva i digitalnih sertifikata koji se nalaze na čipu, i koji pružaju zaštitu ličnih informacija koje se nalaze na kartici i dokazuju autentičnost informacija, onako kako ih je verifikovalo sertifikaciono telo (*certifying authority*).

Verifikovani i autorizovani pristup informacijama. Većina fizičkih i digitalnih identifikacionih karakteristika može biti ostvarena i drugim ID tehnologijama, koje omogućavaju da se informacije jednostavno verifikuju na strani prijema. Uz veliki stepen zaštite informacija i sigurnost, mogućnost smart kartica da obrađuju informacije i reaguju sa svojim okruženjem predstavlja jedinstvenu prednost koju druge tehnologije ne nude. Da bi se neka transakcija odobrila ne moraju sve lične informacije da budu pročitane, npr. za kupovinu alkoholnih pića u nekim zemljama važna je starost osobe, što je samo jedan od ličnih podataka.

Smart kartica je aktivni token. Smart kartica ima mogućnost da pruži informacije koje su potrebne, i to samo onda kad se traže. Jedinstvena mogućnost kartice da verifikuje prava osobe koja zahteva informacije, pruža najbolju zaštitu za lične informacije vlasnika kartice. Personalne ID kartice na bazi smart kartica štite privatnost tako što obezbeđuju odgovarajuću identifikaciju i to zahvaljujući mogućnosti autorizacije i verifikacije pristupa samo onim informacijama zahtevanim u transakciji.

Jaka sigurnost. Smart kartice trenutno predstavljaju najbolji kompromis između sigurnosti i cene. Smart kartice su kompatibilne sa već postojećim sistemima koji koriste kartice - koegzistiraju sa magnetnom trakom, bar kodovima, embosiranim ili samo vidljivo odštampanim na istoj kartici. Kada se koriste u kombinaciji sa drugim tehnologijama kao što su javni ključevi i biometrika, smart kartice je prosto nemoguće duplirati ili falsifikovati, a podaci na čipu se ne mogu menjati bez odgovarajuće autorizacije (*password-i, biometrička verifikacija ili kriptografski pristupni ključevi*).

Isplativa offline verifikacija. Verifikacija bazirana na smart karticama, a uz pomoć malih, sigurnih, jeftinih portabl čitača, može se primeniti na različitim mestima gde se zahteva provera identiteta, kao na primer na aerodromima. Verifikatori potvrđuju identit neke osobe tako što upoređuju skeniranu biometriku sa onom smeštenom na kartici, i na taj način eliminišu potrebu za online pristupom bazi podataka.

Online elektronski potpis (*digitalna identifikacija*). Mnoge zemlje usvojile su zakone kojima se digitalni potpis prihvata kao legalno sredstvo za online poslovanje i razmenu informacija. Smart kartice se smatraju najsigurnijim sredstvom za primenu digitalnog potpisa u infrastrukturi javnih ključeva. Smart kartice mogu da sadrže zaštićene privatne i javne ključeve vlasnika i odgovarajuće sertifikate i da budu u mogućnosti da izvršavaju digitalne kriptografske operacije (*npr. digitalni potpisi*), pri čemu privatni ključ nikada ne napušta operativni sistem koji je na čipu.

Kapacitet za skladištenje informacija. Tradicionalne kartice sa magnetnom trakom imaju ograničen memorijski kapacitet, za razliku od smart kartica, čiji je memorijski kapacitet veliki i varira u zavisnosti od aplikacija. Moguće je imati u jednom sistemu i kartice sa malom memorijom za jednostavne aplikacije i kartice sa velikom memorijom za kompleksne mnogostruke aplikacije. Danas smart kartice nude dovoljno memorije da se smeste komprimovana fotografija, biometrike, digitalni sertifikati i javni/privatni ključevi itd.

Mogućnost pisanja i čitanja. Tehnologija za smart kartice štiti informacije, ali isto tako dozvoljava i promene određenih polja, pod uslovom da podnosilac zahteva autorizuje promenu.

Pošto je upotreba smart kartica tesno povezana sa pitanjima sigurnosti, tipične sigurnosne aplikacije su:

- identifikacija/pristup mreži: kartice sa memorijskim čipom koriste jedinstveni serijski broj kartice za identifikaciju korisnika. Ovo samo donekle obezbeđuje sigurnost, pošto bilo ko ko poseduje karticu može koristiti ovu aplikaciju. Za kompleksnije identifikacione šeme koriste se kartice sa mikrorocerskim čipom.
- sigurnost na mreži: kombinacija smart kartica sa mikroprocesorskim čipom i PKI sistema koristi se za zaštićen prenos kriptovanih podataka. Na kartici se nalaze algoritmi, ključevi i sertifikati neophodni za enkripciju, i kao što smo već rekli ključevi nikada ne izlaze van operativnog sistema same kartice, čime se sprečava upad treće strane u transakciju.
- elektronske finansijske transakcije: koriste se i memorijske i mikroprocesorske smart kartice.

- posebne aplikacije: savremene smart kartice (*Javacard i Personal Computer/Smart Card*) dozvoljavaju programerima da pišu kod za smart kartice, sličan kodu za PC - jeve. Primer su aplikacije za pojavljivanje određene web stranice, po ubacivanju kartice u čitač, aplikacije za pojavljivanje stranice koja je konfigurisana za potrebe korisnika, aplikacije za upisivanje ličnih podataka itd.

Višestruki servisi. Jedna smart kartica može nosiocu da obezbedi pristup različitim ustanovama i organizacijama i njihovim servisima.

Mogućnost povezivanja bez direktnog fizičkog kontakta (*contactless*). Smart kartice podržavaju korišćenje contactless tehnologija, i tako omogućavaju aplikacijama brzu i zaštićenu identifikaciju. Pošto eliminišu potrebu za fizičkim kontaktom, contactless kartice su pogodne za mesta gde se zahteva verifikacija velikog broja identiteta.

1.8.1

PRIMENA SMART KARTICA

Razlikujemo sledeće glavne oblasti primene SMART kartica:

- primena u oblasti državne uprave (*elektronski identifikacioni dokumenti, putne isprave, vozačke dozvole, saobraćajne dozvole, dozvole za nošenje oružja, kartice za socijalnu zaštitu, socijalnu pomoć i penzije, kartice za zdravstveno osiguranje, e-vlada...*),
- komercijalna primena (*bankarstvo - kreditne i debitne kartice, elektronsko bankarstvo, e-poslovanje, e-trgovina, mobilna komunikacija-SIM kartice, transport, TV pretplata, članske karte...*),
- lična primena (*zaštita stanova, kola, mobilnih telefona...*).

U komercijalnoj i oblasti državne uprave informaciona šema za primenu SMART kartice može biti eksterno (*za korisnike komercijalnih usluga, odnosno građane*) ili interno dizajnirana (*službene kartice za zaposlene*).

1.9 ZAKLJUČAK

Zahvaljujući ID karticama moguće je jednoznačno identifikovanje osoba, dokumenata i podataka. Na osnovu ovoga moguće je razviti sistem za personalizaciju ID dokumenata i putnih isprava.

Ovakav sistem omogućava personalizaciju dokumenata zadovoljavajuće pouzdanosti i trajnosti koršćenog materijala (*minimum 10 godina*), kao i visokog estetskog i tehnološkog kvaliteta. Sistem podrazumeva potpunu zaštitu procesa rada dokumenata, zaštitu materijala za izradu dokumenata, kao i zaštitu svih entiteta zasnovanu na infrastrukturi javnih ključeva, certifikatima, digitalnom potpisu i rešenjima na bazi smart kartica.

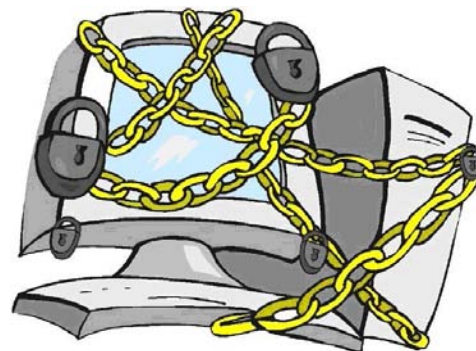
Takođe, sistem omogućava, kroz jednostavniji, pouzdaniji i kvalitetniji rad sa građanstvom, poštovanje međunarodnih normi i standarda. S druge strane nudi sigurno, brzo i efikasno utvrđivanje identiteta lica, kao i zaštitu sigurnosti dokumenata i privatnosti podataka građana.

GLAVA II

2 ZAŠTITA PODATAKA NA PAMETNIM KARTICAMA

2.1 UVOD

Informacione tehnologije danas su primenjene u svim područjima ljudske delatnosti, stvaraju nove vrste poslova i direktno utiču na evoluciju društva. Jedan važan izum objedinjuje i predstavlja sve navedene tehnološke promene, a to je računar.



Prvi računari su bili skromnih mogućnosti, veoma nefunkcionalni i skupi, dok se danas relativno lako može doći do izuzetno moćnih računara. Mogućnosti koje danas računar pruža prosečnom korisniku su do pre desetak godina bile nezamislive. Brzina i stepen razvoja računarskog softvera, ali i pratećeg hardvera je izuzetan. Danas prosečan korisnik u svojoj kući može imati računar koji mu omogućava da profesionalno izrađuje 3D animacije, priprema grafički materijal za štampu, snima i komponuje muziku, pristupa Internetu, komunicira sa udaljenim računarima, obavlja razne vrste plaćanja, naručuje robu itd.

Začetnikom „pametne“ kartice smatra se francuski novinar Roland Moreno koji je 25. marta 1974. registrovao idejne patente pametne kartice. Zbog toga i ne čudi što je prva zabeležena javna primena pametne kartice ostvarena u Francuskoj. Telefonska industrija, odnosno francuski PTT, 1984. izdaje prvu telefonsku karticu. Danas se ona koristi u javnoj telefoniji u više od 50 zemalja širom sveta. Najveće finansijske organizacije: EuroPay, MasterCard, Masters i Visa udružuju svoje napore u cilju primene pametne kartice u finansijskoj industriji. Rezultat je EMV specifikacija izdata 1994. godine. Mobilna telefonija izdaje 1998. GSM specifikaciju koja otvara novo veliko područje primene pametne kartice.

Telekomunikaciona i finansijska industrija predstavljaju najveće sisteme koje koriste pametne kartice. Pametna kartica poseduje velike mogućnosti, a najveće prednosti su njena veličina, prenosivost, dugotrajnost, razne funkcionalnosti i povrh svega, sigurnost. Pomenuta sigurnost predstavlja najvažniju osobinu pametne kartice. Tehnologija danas postaje alat u službi informacije a informacija predstavlja znanje, moć i novac. Sigurno čuvanje informacija i zaštita protoka informacija postaju neophodnost modernog doba. Kao danas najbolje hardversko rešenje se pojavljuje „smart card“. Pametna kartica donosi visok stepen sigurnosti informacije dostupnu svakom, na siguran način čuva informacije i omogućava da se obrada podataka izvodi u sigurnom okruženju.

Najčešći korisnik pametnih kartica sa čipom će biti moderan građanin. Ona će omogućiti njegovu identifikaciju, kao i čuvanje informacija o njegovom finansijskom i zdravstvenom stanju. Potencijalnu opasnost prikupljanja informacija na jednom mestu, predstavlja mogućnost praćenja i upravljanja građanima, o čemu je već bilo javnih rasprava u svetu, ali i kod nas. Dobro osmišljenom eksploatacijom pametnih kartica, pojedinac zadržava u potpunosti svoju privatnost.

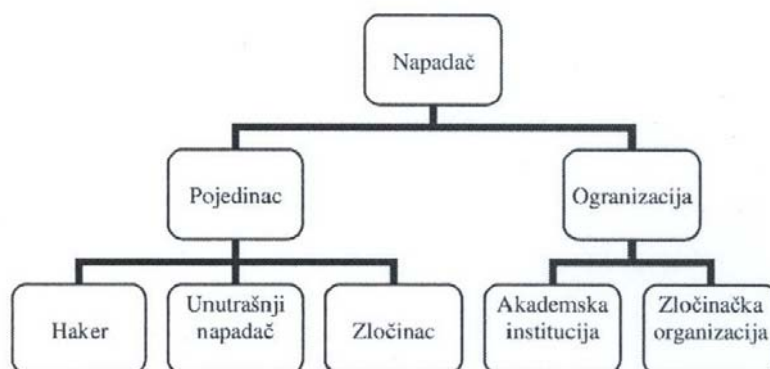
2.2

NAJČEŠI NAPADI NA PAMETNE KARTICE

Mogući su napadi na pametne kartice na nekoliko potpuno različitih načina i nekoliko različitih nivoa. U toku razvoja softvera i hardvera same kartice, neophodno je voditi računa o svim relevantnim potencijalnim slabim sigurnosnim tačkama prikazanim na slikama 10 i 11.



Slika 10 Mogući napadi na čip karticu po nivoima



Slika 11 Klasifikacija mogućih tipova napadača

Svi fizički, logički i sociološki faktori treba da budu uzeti u razmatranje čak i pre početka razvoja pametne kartice. Kartica sa čipom treba da predstavlja sigurnosni hardverski dodatak koji značajno povećava nivo zaštite u prenosu podataka nesigurnim komunikacionim kanalima. Takođe je vrlo važno da se pri projektovanju kartice ili pri njenoj implementaciji tačno odrede potencijalni napadači, kako bi se na odgovarajući način oni preventivno onemogućili.

Mogućnosti napada na pametnu karticu su različiti, a mogu se dogoditi ne samo u eksploatacionom periodu, već i u samom toku njenog razvoja. Poznavanje fizičkog rasporeda komponenti na pametnoj kartici, veštini inženjerima omogućava naknadno očitavanje podataka iz privremene i trajne memorije na kartici.

Zlonamerni programeri koji su učestvovali u razvoju operativnog sistema kartice mogu ostaviti „tajna vrata“ („back door“) u samom softveru. Na taj način, u toku eksploatacije, na samo njima poznat način, mogu doći do podataka koji mogu ugroziti sigurnost koju kartica obezbeđuje.

Na sličan način, stručna lica koja učestvuju u razvoju aplikacije koja će koristiti fizičke potencijale pametne kartice, mogu zlorabiti svoj položaj. Ubacivanjem zlonamernog koda u aplikaciju oni mogu sebi obezbediti nesmetan pristup podacima za koje kartica ima zadatak da ih štiti.

Najčešći metod napada predstavlja napad na logičkom nivou, korišćenjem metode „Brute Force“. Ovaj metod označava pokušavanje napadača da „grubom silom“ otkrije pravu kombinaciju koja može dovesti do dešifrovanja šifrovanih podataka. Ovaj postupak se zasniva na uzastopnom „isprobavanju“ mogućih kombinacija ključa koji bi bio odgovarajući. Ovo „isprobavanje“ kombinacija mogućih šifri se prepušta specijalizovanom softveru koji ima za zadatak da pronade originalni ključ.

Šifre i ključevi koje računarski program za „razbijanje“ zaštite isprobava, obuhvataju sve moguće kombinacije, a u najvećem broju slučajeva, program prati neko pravilo ili redosled karaktera. Program uvek kreće od pretpostavki, pa pokušavanjem probijanja šifre na osnovu njih, dolazi do prave kombinacije. Pošto su današnji računari, čak i kućnog tipa, veoma brzi, probijanje šifri i ključeva koji nisu velike dužine može da traje vrlo kratko, a vreme za to zavisi od više uticajnih faktora. Zavisnost dužine ključa šifrovane poruke od vremena potrebnog za njeno otkrivanje je prikazana u *tabeli 2*.

Simetrični ključ	Asimetrični ključ (RSA, DH,...)
40 bita	274 bita
56 bita	384 bita
64 bita	512 bita
80 bita	1024 bita
96 bita	1536 bita
112 bita	2048 bita
120 bita	2560 bita
128 bita	3072 bita

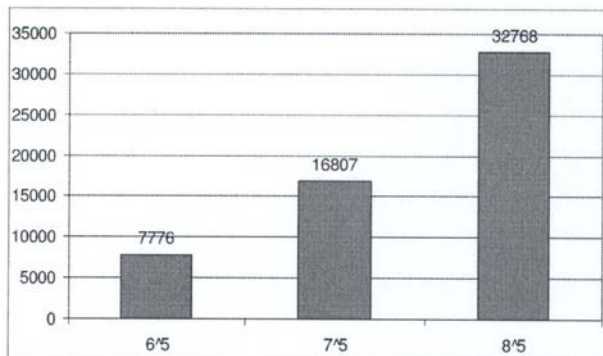
Tabela 2 Standardne dužine ključa

Dužina ključa	Individualni napadač	Mala grupa	Velika kompanija	Vojna obaveštajna služba - sistem
40 bita	nedelje	dani	milisekunde	mikrosekunde
56 bita	vekovi	decenije	sati	sekunde
64 bita	milennijum	vekovi	dani	Minuti
80 bita	nemoguće	nemoguće	vekovi	Vekovi
128 bita	nemoguće	nemoguće	nemoguće	Milennijum

Tabela 3 Potrebno vreme za otkrivanje šifre

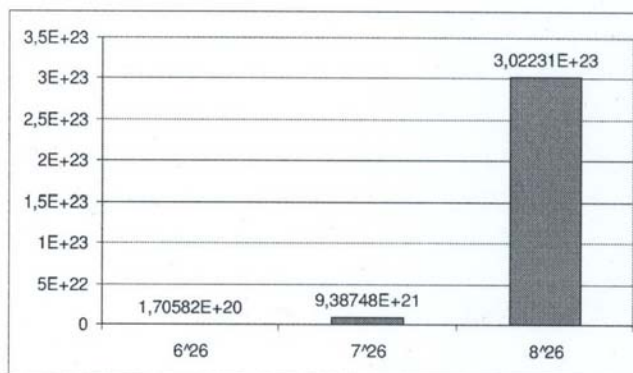
Ukoliko se za šifriranje poruke koristi šifra koja je dužine šest karaktera, a koristi se pet različitih znakova u njoj, broj kombinacija će za ovaj slučaj biti $6^5=7776$. Ovo je broj kombinacija za slučaj da se tačno zna koji su znaci korišćeni u šestoznakovnoj šifri, kao i to koliko znakova šifra u sebi sadrži.

Iz ugla napadača, ovi podaci nisu poznati, pa je tako statistička analiza iz tog ugla potpuno drugačija. Broj kombinacija se menja povećanjem dužine šifre kao na slici 12, ukoliko se ostavi pet različitih znakova u njoj i to: $6^5=7776$, $7^5=16.807$, $8^5=32.768$. Prikazane su vrednosti za dužine šifre od 6, 7 i 8 znakovnih mesta. Iz ugla napadača na šifru ili ključ, situacija je potpuno drugačija



Slika 12 Broj kombinacija šifre vezan za dužinu kjuča

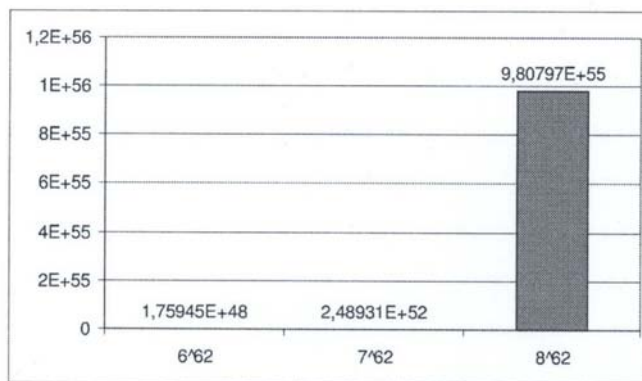
Zakon verovatnoće donosi broj mogućih kombinacija koje napadač treba da isproba, kako bi sigurno otkrio originalnu šifru. Broj kombinacija koje iz ugla napadača on mora da uzme u obzir je prikazan na slici broj 13. U ovom slučaju se podrazumeva da napadač zna da su korišćena samo mala slova engleske abecede (26 slova).



Slika 13 Kombinacije koje napadač mora da „isproba“ u zavisnosti od dužine šifre (za 26 karaktera)

Osoba koja pokušava da otkrije kombinaciju znakova za dešifrovanje originalne poruke ne zna ni koji su karakteri korišćeni u lozinci ili ključu, a ni njegovu dužinu. U ovom slučaju, statističkom analizom dolazimo do mogućih kombinacija koje napadač mora uzeti u obzir.

Za napadača broj 26 označava broj slova koje može uzeti u obzir, ali ukoliko se uzmu u obzir i brojevi i mala i velika slova, broj kombinacija vrtoglavo raste. Za šifru sa 6 karaktera broj kombinacija će u tom slučaju biti 6^{62} , a ne 6^{26} . Za ovakav slučaj je broj mogućih kombinacija šifre ili ključa prikazan na slici 14. Postoji i mogućnost da se zbog povećanja sigurnosti, kao deo šifre uzmu i specijalni karakteri što daje 6^{256} kombinacija.



Slika 14 Broj kombinacija ako su korišćena i velika i mala slova i brojevi bez znakova

Dužina šifre	Iz grupe od 26 karaktera	Iz grupe od 62 karaktera
5 kar.	1 čas i 50 min	6 dana
6 kar.	1 dan i 20 sati	1 godina
7 kar.	46 dana	68 godina
8 kar.	3,3 godine	4.032 godine
9 kar.	90 godina	252.000 godina
10 kar.	2.304 godine	> 1.000.000 godina
16 kar.	1.872.000 godina	> 10.000.000 godina

Tabela 4 Vreme potrebno za otkrivanje šifre na osnovu njene ukupne dužine i korišćenih karaktera (mala i velika slova i brojevi, bez specijalnih karaktera)

Vrednosti u tabeli 4 su prepolovljene od ukupnog vremena potrebnog za isprobavanje svih kombinacija, zbog toga što se uzima za moguće da napadač otkrije pravu kombinaciju pre nego što isproba sve kombinacije.

Vremena potrebna za probijanje šifre su dobijena proračunom i aproksimacijom, ali za računar sledećih karakteristika: Pentium 4 procesor 1600 MHz, 512 MB RAM memorije.

Postoji veliki broj različitih softverskih paketa koji „Brute Force“ metodom pokušavaju da razbiju zaštitu na smart karticama. Sigurno rešenje za neprobojnu šifru ne postoji, ali se dugačkim i šarenolikim (*u smislu korišćenih raznovrsnih karaktera u samoj šifri*) šiframa, teoretski približavamo granici 100% sigurnih šifri. Vreme za njihovo probijanje se smanjuje, kako tehnologija i računarska moć jača, ali je i pored toga sigurnost na izuzetnom nivou ukoliko poštujemo sva preporučena pravila.

2.3 MEHANIZMI ZAŠTITE PODATAKA NA ČIP KARTICAMA

Sigurnost pametne kartice obuhvata četiri komponente, prikazane na slici 15. Telo kartice na sebi sadrži i vizuelne oznake, koje su čitljive čoveku. To su hologrami, reljefna obeležja, ultraljubičasti tekst, laserska graviranja, itd. Tehnike implementacije sigurnosnih obeležja zajedničke su za sve tipove kartica i nisu specifičnost samo pametnih kartica. Preostale komponente - kao što su hardver čipa, operativni sistem i aplikacija, štite podatke i programe mikrokontrolera koji se nalazi na kartici.



Slika 15 Osnovne komponente sigurnosti smart kartice

Mehanizmi zaštite pametnih kartica su mnogobrojni i obuhvataju i hardverske i softverske nivoe njihovog funkcionisanja. U samom postupku razvoja pametne kartice, uvode se sigurnosne mere u cilju obezbeđivanja integriteta podataka na njoj:

- Fizički razvoj mikrokontrolera pametne kartice
 - Razvoj operativnih sistema za pametne kartice
 - Princip podeljenog znanja (*deljenje tajni*)
 - Sigurnost na fizičkom nivou kartice
 - Kodiranje memorije
1. Razvoj mikrokontrolera pametne kartice traje od nedavno. U njemu učestvuju mali broj osoba koji rade u strogo kontrolisanim objektima. Sistemi koji se koriste za razvoj mikrokontrolera su potpuno odvojeni od spoljašnjeg sveta. Dizajn čipa i njegovi mehanizmi zaštite daju se na testiranje nezavisnim organizacijama. Nezavisne organizacije otkrivaju namerne ili nenamerne previde i greške u pogledu sigurnosti, pri čemu smanjuju mogućnost napada iz samog razvojnog sistema. Sam raspored komponenti na čipu je vrlo važan napadačima, ukoliko se odluče za fizičku agresiju na podatke sa kartice.
 - Jedinstveni broj čipa koji se smešta u takozvanu WORM memoriju, uz senzore i zaštitne slojeve, predstavlja hardverski sigurnosni element mikrokontrolera. Često se takva memorija naziva i OTP memorija. Prilikom proizvodnje poluprovodničkog čipa u WORM memoriju se upisuje jedinstveni broj čipa. To znači da svaki čip postaje jedinstven, odnosno može se unutar nekog sistema na nedvosmislen način identifikovati pametna kartica. Broj čipa se koristi u formiranju ključa. Isto tako broj čipa omogućuje generisanje „crne liste“ kartica. Crna lista kartica se koristi za označavanje i uklanjanje sumnjivih kartica iz sistema. Ovaj jedinstveni broj kartice se može uporediti sa MAC adresama računara prisutnih na internetu.
 2. Računari koji se koriste za razvoj operativnih sistema za pametne kartice su u potpuno izolovanoj mreži, bez ikakve mogućnosti spoljašnjeg pristupa. Razvojni alati, kao što su prevodilac i simulator, podvrgnuti su verifikaciji i testiranjima. Za osiguranje ispravnosti prevođenja softvera često se koriste dva različita programera. Po pravilu je zabranjeno i korišćenje softvera nepoznatog porekla.

Vreme razvoja operativnog sistema se može značajno skratiti uvođenjem dodatnih naredbi za svrhu testiranja. Takve naredbe često mogu čitati vitalne delove memorije zaobilazeći sigurnosne mehanizme. Nepažljivošću mogu ostati u operativnom sistemu, što može poslužiti za kasnije napade.

3. Ideja se bazira na činjenici da ukoliko svi učesnici u razvoju sigurnosnih mehanizama jedne kartice znaju sve o njoj, mogućnost za sakrivanje malicioznih činioca je minimalna. Princip podeljenog znanja (*deljenje tajni*) suprotstavljen je principu da svako zna sve o svemu. U razvoju sigurnosnih komponenti ne sme se dozvoliti da kompletno znanje o komponenti pripadne pojedincu, jer bi takav pojedinac bio meta potencijalnog napada. Sigurnosni efekat dobijen deljenjem znanja može se videti po načinu na koji je izvedena poslednja faza implementacije operativnog sistema pametne kartice. U njoj se u EEPROM memoriju učitavaju tablice, programski kod i konfiguracioni podaci. Proizvođač kartica, odnosno proizvođač čipa koji dobija finalni ROM kod za produkciju proizvodnih maski, nema kompletno znanje o operativnom sistemu, jer mu nisu poznati delovi operativnog sistema smešteni u EEPROM-u. Analizom ROM koda ne mogu se u potpunosti otkriti sigurnosni mehanizmi i funkcije operativnog sistema. Na ovaj način je softver potpuno zaštićen od mogućih unutrašnjih napada (*od strane ljudi koji su učestvovali u razvoju kartice*).
4. Postoji nekoliko pravila kojih se proizvođači kartica moraju pridržavati kako bi osigurali neželjene pristupe pametnim karticama. Tehnologija je toliko napredovala da specijalizovane radionice imaju tehničkih mogućnosti da preuzimaju podatke sa delova čipa koji su mikronske veličine. Ovakvih tehnološko opremljenih centara u svetu ima mnogo, a novčani ulazi su ogromni.

U dizajnu čipa pametne kartice zabranjeno je korišćenje standardnih ćelija razvijenih za masovnu proizvodnju poluprovodničkih komponenti, kako bi se sprečilo brzo i lako kopiranje.

5. Najčešće primenjivana metoda zaštite podataka koji se nalaze u radnoj memoriji je kodiranje memorije. Glavna tajna je u metodi i ključu kojim se kodira. Jednostavnim neovlašćenim pristupom memorijskom prostoru, napadač će videti nerazumljive, kodirane vrednosti.

Ključ za kodiranje kartice mora biti jedinstven za svaku karticu ili se čak zasnovati na dinamičkoj izmeni metoda šifrovanja, radi višeg stepena sigurnosti. Što je ključ neobičniji i nedostupniji, podaci su sigurniji. Koriste se i različiti standardni metodi šifrovanja kao što DES⁹, Triple DES, RSA¹⁰ itd.

Podaci u kartici se kodiraju uz pomoć ključeva, u realnom vremenu. Na taj način se originalni tekst sakriva u velikom broju podataka koji su na prvi pogled nečitljivi. Za dekodiranje ovako šifrovanog teksta (*koji može biti kodiran i kombinacijom dva ključa - javnim ključem i tajnim ključem sa kartice*), neophodno je primeniti istu kombinaciju ključeva za dekodiranje. Samo ukoliko je kombinacija ključeva odgovarajuća, informacija se može dešifrovati.

⁹ DES Data Encryption Standard

¹⁰ RSA Rivest, Shamir, and Adleman

2.4 ZAŠTITNA ULOGA SMART KARTICE

Jedna od glavnih uloga smart kartica je zaštita podataka koji se razmenjuju između kartice i čitača. Zaštitom se obezbeđuje tajnost podataka, verifikacija korisnika, verifikacija aplikacije, verifikacija transakcije i neporecivost ličnih podataka i/ili transakcije.

Većina ovih potreba za zaštitom može se zadovoljiti korišćenjem PKI, koji obezbeđuje polise i procedure neophodne za uspostavljanje zaštićene razmene informacija. PKI obuhvata enkripciju podataka, koja obezbeđuje poverljivost, digitalne certifikate, koji obezbeđuju autentičnost, i digitalne potpise, koji obezbeđuju završetak nekog procesa bez promene podataka.

Za proces enkripcije podataka koristimo algoritme - matematičke funkcije koje se koriste za prevođenje podataka u zaštićeni ili enkriptovani format i ključeve - parametri ili brojevi koji se koriste u algoritmima. Enkripcija je proces u kome se koristi algoritam i ključ za kodiranje ili enkripciju podataka, a obrnut proces tj. proces prevođenja enkriptovanih podataka u originalni oblik je dekripcija.

Primena elektronskog identifikacionog dokumenta mora da osigura:

- **Pouzdanu verifikaciju** korisnika, aplikacija, transakcija, odnosno da osigura da samo ovlašćena lica pristupaju važnim podacima ili da vrše obradu podataka,
- **Tajnost**, odnosno **poverljivost podataka** odnosno da lični i poverljivi podaci budu zaštićeni od neovlašćenih pristupa,
- **Integritet podataka** odnosno da nije moguće bilo kakvo menjanje podataka od strane neovlašćenih lica,
- **Raspoloživost podataka** odnosno da su oni dostupni ovlašćenom licu ili aplikaciji kad god je to potrebno.

Svakom od ovih zahteva udovoljava se različitim sigurnosnim merama (*pouzdana verifikacija se postiže korišćenjem lozinke, PIN-a ili biometrike - otiska prsta*), tajnost podataka se može osigurati enkripcijom podataka, očuvanje integriteta korišćenjem **hash** algoritama i dr.

Izbor sigurnosnog mehanizma zavisi od namene ITS (*za kućnu primenu računara dovoljan sigurnosni mehanizam za verifikaciju korisnika će biti korisničko ime i lozinka*). Složeniji informaciono telekomunikacioni sistema (*slučaj eID*) mora imati optimalnu kombinaciju različitih sistema zaštite.

Za sada, najnapredniji sistem zaštite pruža kombinacija pametnih kartica, biometrijskih podataka vlasnika kartice i infrastrukture javnih ključeva.

2.5 SIMETRIČNE I ASIMETRIČNE ENKRIPCije

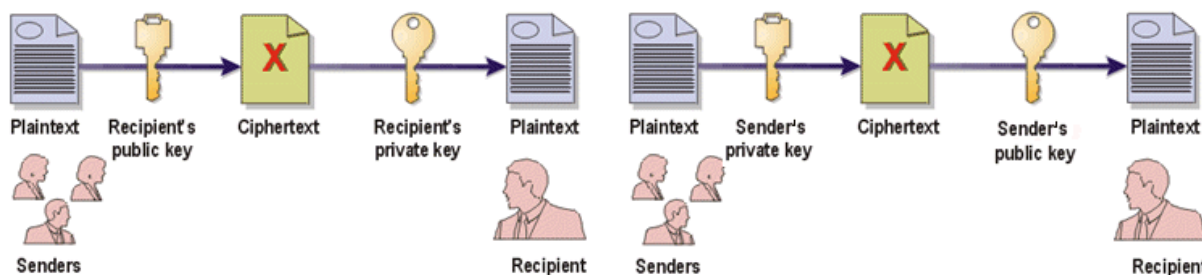
2.5.1 Put do sigurnih podataka

Iako verovatno ne znaju za sam termin PKI, mnogi naši sugrađani su trenutno u velikoj nedoumici da li da se protive ili ne primeni ove tehnologije u svakodnevnom životu - pogađate, reč je o novim ličnim dokumentima koji, umesto u papirnoj formi, sada se izdaju u obliku plastičnih kartica sa čipom. Brojne kritike upućene na račun novih medija delimično su posledica neobaveštenosti i pogrešnog razumevanja tehnologije koja zapravo donosi mnogo dobrih stvari, ali kod koje treba ozbiljno razmatrati i bezbednosne rizike.

Sve je počelo šifrovanjem, jer otkad postoji komunikacija među ljudima prisutna je i želja da se neke informacije sakriju. Iako su u te svrhe razvijane nebrojene tehnike, najpoznatija su rešenja koja smislenu informaciju teže da pretvore u besmisleni, koju će primalac primenom nekog postupka opet pretvoriti u smislenu. Postoje dve grupe mehanizama za ove postupke, a to su (*ako izuzmemo analogne metode, kao što je spiralno namotavanje trake papira na štap i pisanje po njemu*) simetrični i asimetrični.

Algoritmi su simetrične ili nesimetrične matematičke funkcije koje se koriste za enkripciju i dekripciju podataka. Simetrične funkcije koriste privatni ključ za enkriptovanje i dekriptovanje podataka. Privatni ključ se šalje primaocu što predstavlja sigurnosni rizik. Bilo ko, ko poseduje privatni ključ može pročitati enkriptovane podatke. Simetrične funkcije mogu biti pogodne za jedan - na - jedan transakcije, ali ne obezbeđuju dovoljno sigurnosti kada se podaci prenose preko mreže. Najpoznatiji simetrični algoritam je DES¹¹ i unapređena verzija 3DES. Za realizaciju web zaštite potrebno je koristiti minimum 3DES algoritam, bez mehanizma za rekonstrukciju ključa ili realizovati sopstveni sistem zaštite na kombinaciji simetričnog i asimetričnog algoritma.

Asimetrična kriptografija koristi algoritam koji koristi javni i privatni ključ, kao što je prikazano na slici 16.



Slika 16 Primer asimetrične kriptografije

Kod asimetrične kriptografije imamo dva slučaja. U prvom slučaju pošiljalac mora da:

- Enkriptuje podatke korišćenjem javnog ključa primaoca
- Pošalje podatke primaocu

¹¹ DES - Data Encryption Standard

S druge strane primalac mora da:

- Primi enkriptovane podatke od pošiljaoca
- Dekriptuje podatke korišćenjem svog privatnog ključa

Na ovaj način je ostvarena tajnost komunikacije između pošiljaoca i primaoca poruke. Pošto je javni ključ primaoca svima poznat, primalac ne može biti siguran ko mu je poslao poruku.

U drugom slučaju pošiljalac mora da:

- Enkriptuje podatke korišćenjem svog privatnog ključa
- Pošalje podatke primaocu

S druge strane primalac mora da:

- Primi enkriptovane podatke od pošiljaoca
- Dekriptuje podatke korišćenjem javnog ključa pošiljaoca

U ovom slučaju pošiljalac je poznat, i ostvarena je neporecivost, ali nije ostvarena tajnost komunikacije, jer bilo ko, ko zna pošiljaočev javni ključ može da dekriptuje poruku.

Kriptografija sa javnim ključem ima ograničenje u nedostatku brzine; najbrže primene asimetričnih kriptografija su mnogo sporije od tipičnih primena simetričnih kriptografija.

Postoji nekoliko algoritama u upotrebi za kriptografiju sa javnim ključem, u zavisnosti od zahtevanog nivoa zaštite. RSA¹², nazvan po svojim pronalazačima, i ECC¹³ su primer dva široko korišćena algoritma koji zadovoljavaju većinu zahteva za javnim i privatnim ključevima.

2.5.2

Simetrično...

Stotinama godina je postojala samo grupa koja je koristila simetrične postupke (*algoritme*). Primer ovakvog postupka predstavlja „pomeranje“ slova, kada se svako slovo menja onim koje je npr. pet mesta dalje u abecedi - slovo A bi menjali sa F, B sa G itd. Pošiljalac bi svoju poruku šifrovao pomeranjem slova naviše, a primalac dešifrovao pomeranjem naniže. Da bi primenili algoritam, pošiljalac i primalac informacije moraju da dele neku tajnu informaciju koja omogućava pravilnu transformaciju u oba smera, a koja se naziva „ključ“.

U ovom primeru to je veličina pomeraja (*5 slova*). Za razliku od primera sa prostom substitucijom, postoje sofisticirani algoritmi koji vrše simetričnu zaštitu podataka, kao što su DES (*koristi ga i SSL*), IDEA i AES (*novi standard koji će zameniti DES*), koji imaju jako široku primenu.

¹²RSA - Rivest-Shamir-Adleman

¹³ECC - Elliptic Curve Cryptography

Prednost ovakvog algoritma je brza implementacija, pa je samim tim on pogodan za rad sa velikim količinama podataka, kao i sa podacima koji stalno „teku“ (*npr. veza između dve mreže*). U mane prvenstveno spada neophodnost razmene „tajnog ključa“ između strana koje komuniciraju, koja lako može izazvati probleme - za razmenu je potreban poseban sigurni kanal, koji često nije moguće napraviti.

Ako neko tokom razmene dođe do tajnog ključa, imaće pristup svim šifrovanim informacijama. Jedan od velikih problema prilikom razmene ključeva nastaje i ako se dve strane koje su uključene u razmenu međusobno ne poznaju, pošto se neko treći može lažno predstaviti i tako doći do „ključa“. Dodatnu ozbiljnu manu predstavlja i broj tajnih ključeva i njihovo održavanje, kada je potrebno da jedna strana ostvari zaštićenu komunikaciju sa više međusobno nezavisnih drugih strana, kojih može biti mnogo.

Broj ključeva za involviranih n strana koje međusobno komuniciraju je $n^2 / 2$, dakle za samo 100 učesnika je potrebno oko 5000 tajnih ključeva! Problem njihovog održavanja se dodatno produbljuje ako ključevi imaju ograničeno trajanje (*što je značajno za sigurnost*), pa se periodično menjaju.

Postoji više rešenja ovog problema, a jedno je upotreba centralnog servera za ključeve, koji treba da bude dobro zaštićen i stalno na raspolaganju (*on-line*), jer u suštini vrši „upoznavanje“ strana koje komuniciraju. Ako server ne funkcioniše ili bude kompromitovan, čitav sistem pada. Ali, on predstavlja i cilj prilikom napada na sve učesnike odjednom, a komplikovano je i ostvarivanje komunikacije sa entitetima van osnovnog skupa učesnika.

2.5.3

...ili asimetrično

Sredinom sedamdesetih godina prošlog veka istraživači Whitfield Diffie i Martin Hellman su osmislili način šifrovanja podataka koji se fundamentalno razlikuje od simetričnog. U ovom sistemu postoje dva različita ključa koji su u izvesnoj matematičkoj vezi, od kojih jedan služi za šifrovanje a drugi za dešifrovanje informacija. Ovi ključevi su toliko različiti da je praktično nemoguće da se „za života korisnika“ iz jednog izvede onaj drugi, mada je to teorijski izvodljivo. Tako nećete kompromitovati bezbednost komunikacije čak ni ako javno publikujete ključ za šifrovanje (*na primer na Internetu, u telefonskom imeniku, na vizit-karti*), a za sebe sačuvate samo ključ za dešifrovanje.

Svedeno na jednostavnije izraze, svako ko želi da npr. meni pošalje zaštićenu poruku moći će da je šifrue koristeći moj javni ključ, a samo ću ja moći da je dešifrujem upotrebom svog privatnog ključa (*koji ne treba mešati sa tajnim ključem koji se primenjuje u simetričnoj kriptogranji*). Čak ni sam pošiljalac više neće moći da dešifruje sopstvenu poruku.

Kada se pojavio, rad ove dvojice naučnika je bio toliko radikalno nov i zanimljiv da je stimulisao intenzivna istraživanja na tom polju, koja se i dan - danas nastavljaju. Tako su stvorene mnoge vrlo dorađene implementacije kroz algoritme (*za neke se ipak ispostavilo da nisu dovoljno sigurni*), koje predstavljaju daleko najsigurniji metod zaštite prilikom razmene informacija. Ceo ovaj domen je postao poznat pod nazivom Public Key Cryptography i danas ima široku primenu.

2.5.4

Imenik kome (ne) verujemo

Otkriće metoda za kriptogradnju javnih ključeva je omogućilo unapređenje nekih postojećih, ali i pojavu novih servisa koji ranije nisu bili izvodljivi. Jedna od najvažnijih prepreka koje su mučile simetričnu kriptogradnju jeste nemogućnost kreiranja sigurne komunikacije između osoba koje se prvi put susreću. Novi sistem omogućava slobodno objavljivanje javnih ključeva, pa ako Alis hoće da pošalje zaštićenu poruku Bobu (*Alis i Bob su uobičajena imena za strane u kriptografskim primerima*), pronaći će njegov javni ključ u nekom javnom direktorijumu (*npr. telefonskom imeniku*) i upotrebiti ga za zaštitu.

Tu leži jedna moguća zamka - Alis nekako mora da zna da ključ koji preuzima zaista pripada Bobu, a ne nekom ko se samo predstavlja kao Bob. Postoje dva mehanizma za tu potvrdu. Prvi je da Alis veruje imeniku sa informacijama, kao kada gledate u telefonski imenik. Kod papirnih dokumenata to je sasvim prihvatljivo, jer je mala šansa da će vam neko upasti u kuću kako bi u imeniku nekako menjao brojeve. U digitalnom svetu to može predstavljati veliki problem i elektronskim imenicima se generalno ne može mnogo verovati. Zato je drugi metod neuporedivo bolji, a on podrazumeva da Alis može da proveriti informaciju, što čini suštinsku razliku i donosi neverovatan kvalitativni skok. Dakle, sama informacija mora biti nezavisno „proverljiva“.

Uobičajeni mehanizam za ovaj postupak uključuje upotrebu sertifikata javnog ključa, popularnije nazvanog digitalni sertifikat. Digitalni sertifikati su javno dostupni.

Simetrični i asimetrični mehanizmi, dakle, zahtevaju neko telo koje će „upoznati“ stranke. Razlika je u tome što je u domenu simetričnog šifrovanja tajnost podataka od krucijalne važnosti - ako neko uspe da se domogne tajnih ključeva, čitav sistem je kompromitovan. Kod asimetričnog šifrovanja tajnost je nebitna - napadač mora da ostane neopažen dok eksplicitno manipuliše podacima, što nije nimalo lak zadatak.

Algoritmi za šifrovanje asimetričnim ključevima su u načelu za par redova veličine sporiji od algoritama za šifrovanje simetričnim ključevima, pa mogu biti nepraktični za upotrebu. Stoga se vrlo često koristi kombinacija ova dva metoda.

Pošiljalac generiše slučajan simetrični ključ, kojim se šifruju podaci. Taj ključ (*koji je srazmerno mali u odnosu na podatke koji se prenose*) se šifrjuje javnim ključem primaoca, i sve se to pošalje primaocu. Primalac prvo dešifrjuje simetrični ključ svojim privatnim ključem, a zatim dobijenim simetričnim ključem dešifrjuje same podatke - u suštini jednostavno.

Na ovaj način se objedinjuju najbolje strane oba koncepta, a simetrični ključ se ponovo generiše za svaki prenos informacija te nema potrebe da se negde čuva, što prirodno isključuje opasnost od krađe. U ovim slučajevima, simetrični ključ se naziva još i sesijskim ključem, jer mu rok trajanja ističe nakon jedne sesije.

2.6 IDENTIFIKACIJA PUTEM RADIO FREKVENCije

2.6.1 Zaštita privatnosti i bezbednost podataka

Osnovni problem u razvoju RFID¹⁴ rešenja su pitanja privatnosti (*poverljivosti*) i bezbednosti podataka. Ova pitanja, iako povezana, su različita. Osvrćući se na RFID tehnologiju, definišemo pojmove poverljivosti i bezbednosti na sledeći način:



- **Poverljivost RFID sistema** je osobina sistema da zaštiti značenje informacije prenesene između taga i RFID čitača zaštićenom od primaoca RF signala kome informacija nije namenjena.
- **Bezbednost RFID sistema** je osobina sistema da zaštiti svaku informaciju prenesenu između taga i RFID čitača od primaoca RF signala kome informacija nije namanjena.

Ova dva pojma imaju veoma različite posledice i različita rešenja. U datom okruženju, neko RFID rešenje može imati sigurnosne rizike bez uticaja na poverljivost. Jedan primer ovakvog scenarija je kada tag emituje svoj jedinstveni identifikacioni broj u postojanom ali nekriptovanom obliku. To omogućava da tag bude detektovan od strane bilo kog čitača koji može dekodirati RF signal. Ako je jedino što se može pročitati jedinstveni identifikacioni broj bez mogućnosti da se zaključi šta taj identifikator znači bez pristupa bazi podataka u pozadini, to onda odražava odnos između identifikatora taga i objekta koji on predstavlja kao odnos bez poverljivosti podataka. Bez obzira na to, praćenje i popis resursa ili robe može da postoji.

Praćenje i popis resursa robe su u relaciji sa mogućnošću da neautorizovano lice pročitati identifikatore poslate RFID tagom bez potrebe da zna šta je datim tagom obeleženo ili ko i šta ga nosi sa sobom. Drugim rečima samim obuhvatanjem signala emitovanim od strane RFID taga, neko može pratiti gde je tag trenutno ili gde je prethodno bio kao i o tome koji tagovi su detektovani a koji ne.

Standardni EPC tag prenosi informaciju povezanu sa odgovarajućim proizvodom, odgovarajućim modelom ili klasom proizvoda kojoj pripada i proizvođačem koji ga je proizveo.

Bilo ko sa standardnim EPC čitačem može se približiti dovoljno blizu kupca, da odredi koji proizvode i u kojim količinama on kupuje. Još dalje od toga, neautorizovani čitač može pratiti kupca i iz veće daljine korišćenjem čitača veće snage.

¹⁴ RFID - Radio Frequency Identification

2.6.2

Pitanje poverljivosti

RFID je odlična tehnologija za praćenje objekata. U ovom slučaju možemo definisati neki objekat kao fizički inventar koji ima tri dimenzije. To znači da položaj bilo kog fizičkog objekta (*uključujući i živa bića: životinje i ljude*) potencijalno može biti praćen u okviru područja RFID infrastrukture. Kako razvoj RFID tehnologije napreduje, područje delovanja će postati sve šire i šire.

Ova činjenica je podstakla mnoga pitanja i interesovanja ljudi zbog potencijalne invazije privatnosti informacija koja može biti pripisana RFID tehnologiji. Ali, pre nego što dublje uđemo u pitanje poverljivosti i posledice toga, pogledajmo par primera šta zaštitnici privatnosti i javnost ukazuju da može biti pogrešno u upotrebi RFID tehnologije.

2.6.3

Praćenje putnika putem pasoša koji nose

Vlada Sjedinjenih Američkih Država je donela odluku da ugradi bezkontaktne čipove u pasoše svojih državljana. Ovi čipovi sadrže informacije o vlasniku pasoša kao i njegovu digitalnu fotografiju. U početku, američka administracija nije uključivala nikakve zaštitne protokole. Informacije bi ostale nekriptovane u čipu pasoša. Tako bi svako sa odgovarajućom tehnologijom za čitanje mogao skenirati pasoš putnika, možda dok je pasoš još kod samog putnika, i dobiti lične podatke. Ovo bi, smatraju neki, moglo pomoći teroristima, lopovima ili nekim drugim zlonamernim ljudima da utvrde identitet putnika ili njegovu nacionalnost.

Nakon mnogo negativnih reakcija javnosti i raznih društvenih organizacija američki državni organ promenio je zahtev i dodao 3 nivoa zaštite:

- **Enkripcija:** Informacije u RFID čipu će biti kriptovane.
- **Kontrola pristupa:** Ključ za dekriptovanje podataka će biti kodiran u pasošu i moći će da se dobije samo skeniranjem pasoša optičkim čitačem, čitač pasoša će tek nakon toga moći da dekriptuje podatke korišćenjem tog ključa.
- Korice pasoša će sadržati metalnu mrežu koja će formirati Faradejev kavez koji će sprešiti čitanje RFID čipa kada je pasoš zatvoren.

Eksperti za bezbednost još uvek raspravljaju o ovom pitanju raspravljajući o činjenici da jedinstveni identifikator u čipu može biti pročitao bilo kojim čitačem što je niži nivo zaštite od onog koji omogućava metodologija enkripcije. To takođe otvara i pitanje praćenja pasoša.

2.6.4

Teorija zavere

Najupućenije grupe ljudi koje se bave pitanjem zaštite privatnosti, tvrde da vlasti potencijalno mogu dobiti pristup svim komercijalno kontrolisanim RFID bazama podataka i tako dobiti potpun pristup informacijama o potrošnji, putovanjima i generalnim navikama svoje populacije. Takođe, vlasti mogu dobiti ove informacije postavljanjem RFID infrastrukture širokog opsega gde bi se mogle pratiti sve aktivnosti građana, od toga šta kupuju, šta čitaju, gde putuju do toga šta gledaju na svojim ekranima.

Na početku, komercijalne RFID aplikacije nisu uključivale zaštitu. RFID čitači i tagovi komunicirali su jedni sa drugima koristeći otvorene, nekriptovane poruke, čak i danas, većina RFID čitača i tagova emituju informacije bez bilo kakve enkripcije.

Postoji nekoliko razloga zašto je to tako:

- Korišćenje RFID tehnologije je donekle ograničeno specijalizovanim aplikacijama.
- U bliskoj budućnosti, vodeće implementacije RFID tehnologije će biti u okvirima lanaca snabdevanja
- RFID tagovi, da bi bili što jeftiniji, dizajnirani su sa vrlo ograničenom procesorskom snagom, što otežava uvođenje algoritama enkripcije ili usložnjava prenosne elektronske sklopove unutar tagova.
- Većina današnjih RFID implementacija još uvek radi na nivou praćenja kutija ili paleta, ali ne i na nivou pojedinačnih pakovanja
- RFID infrastruktura je skupa i komplikovana za ugradnju. Obično pokriva veoma ograničenu površinu i time stvara prirodnu odbojnost za široko korišćenje u špijunske svrhe.

Osnovni problem u stvaranju razvijenog RFID tržišta je to što je najčešći zadatak da se cena infrastrukture svede na minimum. To utiče na ograničenje složenosti tagova, pa tako i njihove sposobnosti da obrađuju informacije. Stoga pitanje kako stvoriti bezbednu RFID infrastrukturu ostaje, za sada, u drugom planu.

2.7 RFID metode zaštite

Do sada je bilo mnogo predloga sa ciljem stvaranja sigurnog RFID okruženja. Neki od njih se baziraju na algoritmima enkripcije, neki na pametno dizajniranim komunikacionim šemama, a drugi unapređenjem osnovnih fizičkih karakteristika RFID komunikacije.

2.7.1 Faradejevi kavezi

Ovo je relativno tehnološki nizak nivo pristupa pitanju RFID bezbednosti. Faradejevi kavezi se baziraju na principu mreže od odgovarajućih metala koja stvara prirodnu barijeru radio talasima. Međutim, taj princip stvara novi izazov za razvoj RFID aplikacija. U isto vreme dok je veoma efikasno, ovo rešenje zahteva promišljene, manualne radnje kojima korisnik mora pokriti ili otkriti tag svaki put kada želi da tag funkcioniše. Ova metoda ne nudi nikakvu zaštitu kad je tag van Faradejevog kaveza.

Ipak, ima aplikacija gde Faradejev kavez ima smisla. Korišćenje Faradejevog kaveza kao korice pasoša verovatno radi dobro za većinu korisnika s obzirom da se pasoš obično otvara samo onda kada ga treba pokazati. Za tagove na proizvodima, Faradejev kavez je skupo rešenje.

Ovaj metod se bazira na redukciji RF signala tako da se on prostire svega nekoliko santimetara. Osnovna pretpostavka je da tuđi, neplanirani čitač treba da bude vrlo blizu tagu, a time postaje lako uočljiv. Zapravo, ovo je vrlo slab metod za sigurnu zaštitu. Zamislite osobu koja nosi proizvode sa RFID tagovima ograničenog dometa u popodnevnom špicu na autobuskoj stanici ili metrou. Prosto je nemoguće da izbegne zlonamerne osobe koje nose RFID čitače u njegovoj blizini.

2.7.2 Naredba KILL

KILL naredba čini tag nečitljivim. Ovo je naredba ugrađena u čip RFID taga koja se može aktivirati iz čitača i na mestu prodaje. Da bi izvršio KILL naredbu, čitač mora preneti odgovarajući PIN kod kako bi se osiguralo da zaista ima dozvoljen pristup određenom tagu.

Iako je veoma efikasna, kada se naredba uspešno izvrši, nastaju dva glavna ograničenja:

- Nema efekta sve dok se naredba ne izvrši. To znači da mora biti kombinovana sa nekim drugim rešenjem da bi se obezbedila zaštita tokom celokupnog veka jednog taga.
- To sprečava korišćenje taga u narednim aplikacijama nakon što je proizvod prodan.

Iako ovo nije najtragičniji scenario koji se može zamisliti, on dovoljno ilustruje problem. KILL naredba može ozbiljno ograničiti RFID funkcionalnosti i RFID aplikacije nakon trenutka prodaje.

2.7.3

Naredba SLEEP

Korišćenje ove naredbe na tagovima je pokušaj da se da odgovor na mane koje nosi upotreba naredbe KILL. SLEEP naredba je stvorena kao daleko komercijalno prihvatljivo rešenje. Umesto uništavanja taga na mestu prodaje, ovo rešenje čini tag privremeno neaktivim, sve dok korisnik fizički ponovo ne aktivira tag. Međutim, činjenica da tag treba da omogući korisniku da ga reaktivira stvara nove probleme. Na primer, zamislimo da nakon kupovine odeće umesto da odmah koristimo prednosti RFID mašine za veš, moramo prethodno fizički da reaktiviramo svaki RFID tag ponaosob.

2.7.4

Deljivi tagovi („Clip Tags“)

Ovaj pristup, predstavljen od strane IBM-a, pruža pristojno jednostavno, još uvek efikasno rešenje da bi se smanjilo prepoznavanje tagova sa standardne daljine čitanja. Ova procedura koristi tag sa antenom koja se može odseći u trenutku prodaje u cilju skraćivanja antene i time smanjenja dometa čitanja sa nekoliko metara na jedan do dva santimetara.

Kao što se vidmo, ima mnogo izazova u stvaranju sigurnog i poverljivog RFID rešenja. Postoji, ipak, mnoštvo različitih tehnologija i mehanizama razvijenih u cilju pomoći proizvođačima i korisnicima. Svakako, mi smo tek na početku razumevanja problema i rešenja ovog komplikovanog tehnološkog i društvenog pitanja.

2.8 Mogući napadi

Pre nekoliko godina Lucas Grunwald je uspeo da prekopira sadržaj čipa iz jednog e-pasoša u drugi takav čip, što je izazvalo zgražavanje javnosti, deklarirajući elektronske pasoše „propalom pričom“. Nažalost, niko se od novinara nije potrudio da dublje ispita problem - informacije koje su potrebne da se tako nešto uradi su javno dostupne na Internetu, ali treba znati da primarna namena čipa nije sprečavanje čitanja (*i kopiranja*) njegovog sadržaja, već sprečavanje neopažene promene podataka i samim tim falsifikovanje pasoša, za šta služi digitalni potpis. Grunwald jeste uspeo da prekopira sadržaj, ali ne i da ga izmeni - kakva onda korist od toga, kad će granično osoblje, pri skeniranju pasoša, videti različite štampane podatke (*niko nije pominjao da je to ekstremno teško da se uradi*) i one koji su u čipu, i samim tim odmah znati da pasoš nije validan.

Mehanizam koji omogućava proveru ispravnosti dokumenata koje je izdala jedna država od strane druge države postoji, a to je javni registar ključeva (*Public Key Directory, PKD*). Da ne ulazimo u tehničke detalje, PKD omogućava da se bilo koji elektronski pasoš na bilo kojoj tački u svetu nepogrešivo kontroliše na ispravnost, proverom digitalnog potpisa podataka i lanca sertifikata do državnog tela koje ga je izdalo. Do sada je PKD-u pristupilo deset država, od kojih ga aktivno koristi samo pet, mada će taj broj rapidno rasti u sledećih par godina jer se mnoge zemlje pripremaju za njegovu primenu.

Da tamo gde PKD (*još uvek*) nije primenjen postoji prostor za malverzacije nedavno je demonstrirao Jeroen van Beek, koji je uspeo da izmeni sliku na samom čipu, uz kreiranje digitalnog potpisa koji je zvaničan ICAO alat za proveru elektronskih podataka pasoša, Golden Reader Tool, „progutao“ kao ispravan. Međutim, pored neminovnog dolaska PKD-a, „zaboravljeno“ je i to da treba neopaženo izmeniti i sliku na glavnoj strani pasoša da bi sve to imalo nekog smisla, što je samo po sebi problem.

Svi ovi problemi su poznati odavno, a sada počinje da se uvodi i napredniji način komunikacije sa čipom elektronskog pasoša, nazvan Extended Access Control. EAC ima drugačiji način pristupa snimljenim podacima od BAC-a i koristiće se za čitanje „osetljivih“ podataka kao što je otisak prsta. Osnovna razlika je da se i čitač mora pravilno predstaviti pasošu da bi se sprečio skimming, tj. upotreba neovlašćenih uređaja. Neophodno je i da bude implementiran lanac poverenja kroz posebne digitalne sertifikate, koji se za razliku od mehanizma PKD-a realizuje direktno između svih parova zemalja. Razlika je i u tome što PKD radi sa standardnim X.509 digitalnim sertifikatima, a EAC sa CV¹⁵ sertifikatima koji su mnogo kompaktniji, pa samim tim zgodniji za male memorijske prostore i sporu komunikaciju. Za sada ga je uvela Nemačka, ali će i druge EU države do kraja 2009. morati da ga primene.

Srbija nema mnogo izbora u smislu primene novih elektronskih pasoša - ceo razvijeni svet je već krenuo u tom smeru, pa moramo i mi, hteli - nehteli. Ne smemo iz vida ispustiti suštinu, a to je da putna isprava ima za cilj ne samo da identifikuje pojedinca, već i da spreči krađu identiteta, tj. falsifikovanje. S obzirom na složenost postupka uvođenja (*svaka država ima svoje procedure*), kompatibilnost sa postojećim sistemom rada i neophodnost da sve države sveta obezbede brz i siguran mehanizam provere ispravnosti, nije neobično da će ceo proces trajati barem deceniju. Kada bude završen, prelazak preko granice biće neuporedivo lakši i brži nego sada.

¹⁵ CV - Country Verifiable

2.9 ZAKLJUČAK

U ovom delu su opisani najčešći napadi na pametne kartice, kao i mehanizmi zaštite podataka koji se nalaze unutar tih kartica. Pametne kartice su danas izuzetno dobro zaštićene, ali i pored toga se radi na daljem razvoju i usavršavanju tehnologija i mehanizama zaštite koji bi dodatno onemogućili napadače.

U cilju ostvarenja zaštite visokog nivoa, pored primene zaštite na više nivoa i kombinovanja različitih tehnika zaštite potrebno je i da proizvođači pametnih kartica uzmu u obzir sve moguće poznate, kao i da predvide za sada nepoznate vrste napada i da ih unapred onemoguće.

GLAVA III

3 BIOMETRIJSKE METODE U AUTOMATSKIM SISTEMIMA ZA IDENTIFIKACIJU I VERIFIKACIJU OSOBA

3.1 UVOD

U današnje vreme vladama i raznim organizacijama širom sveta potrebna je isplativa i pogodna kontrola i administracija populacijom, koja mora ujedno da obezbedi i visok nivo zaštite privatnosti podataka i sprečavanje neovlašćenog pristupa. Identifikacija populacije je temelj nacionalne sigurnosti. S druge strane javnosti je potrebna pogodna, sigurna i zaštićena verifikacija ličnog identiteta, što jeftinija i dostupnija usluga i vrlo visok stepen sigurnosti prilikom skladištenja i korišćenja ličnih podataka.

Potreba za identifikacijom ljudi javila se davno. Kroz istoriju postojali su razni primeri registara i identifikacionih dokumenata razvijanih za potrebe identifikacije ljudi. Tako je, na primer, pasoš kao sredstvo za identifikaciju poznat u Engleskom pravu još od 1300. godine.

Identitet neke osobe možemo iskazati na različite načine:

- izgled (*kako osoba izgleda, pol, visina, težina*)
- ime (*kako se osoba zove, nadimak*)
- kôd ili šifra (*obeležje pridodato od strane organizacije*)
- znanje (*odredjene lozinke, podaci*)
- vlasništvo (*dokumenta za identifikaciju*)
- zvanje (*čime se osoba bavi*)
- biometrika (*biološki podaci i ponašanje*)

3.2 BIOMETRIJSKI STANDARDI I METODE

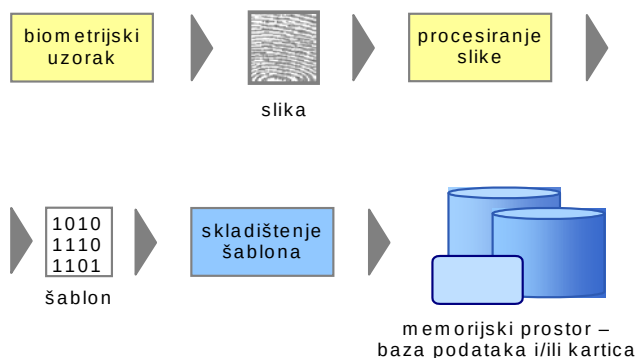
Pored definisanja identiteta neke osobe, potrebno je razviti i načine za utvrđivanje identiteta, odnosno verifikaciju osobe. Cilj verifikacije je da zaštiti sistem od neautorizovanog korišćenja. Procedura se bazira na sledećim načelima:

- **Dokaz po znanju:** Verifikacija se vrši pomoću unapred zadatih informacija kojima određena osoba raspolaže (*lozinka, personalni identifikacioni broj - PIN...*).
- **Dokaz po posedovanju:** Osoba se autentifikuje pomoću posedovanja objekta (*npr. putna isprava, lična karta, magnetna kartica, smart kartica...*)
- **Dokaz po osobinama:** Vrši se merenje osnovnih ljudskih karakteristika (*biometrika*).

Razvoj informatičko - komunikacionih tehnologija pruža nove i kvalitativno napredne mogućnosti za poboljšanje sistema za identifikaciju i verifikaciju korisnika. Finansijske ustanove prve su počele da primenjuju nova rešenja. Informatičke kompanije širom sveta su razvile sisteme za digitalnu verifikaciju u elektronskom poslovanju, po načelima znanja i posedovanja. Veoma brzo ove metode pokazale su nedostatke, što je dovelo do lažnog identifikovanja i raznih drugih tipova zloupotreba; dešava se da ID kartica bude ukradena, lozinka ili PIN broj zaboravljeni i slično. Kod ovakvih sistema nivo zaštite i kompleksnost rešenja direktno su proporcionalni. Proces verifikacije može se olakšati korisnicima ukoliko se kroz različite sisteme koristi ista kartica, PIN broj ili lozinka, ali na taj način smanjujemo sigurnost procesa verifikacije.

Sistem koji omogućava najjednostavniju i najsigurniju verifikaciju i/ili identifikaciju je biometrika. Ona se ne bazira na nečemu što pamtim (*PIN, lozinka ...*), ili nečemu što posedujemo (*papirni dokument, magnetna kartica, smart kartica ...*), već na onome što jesmo. Biometrički sistem za verifikaciju i/ili identifikaciju posmatra osobu analizirajući njene fizičke osobine ili ponašanje.

Verifikacija podrazumeva proveru **1:1** - određena karakteristika osobe poredi se sa referentnim podatkom koji odgovara identitetu za koji osoba tvrdi da je njen (*fotografija na dokumentu sa licem osobe, korisničko ime i lozinka, PIN...*). Identifikacija je provera **1:n**, što znači da se u nekom sistemu identitet osobe proverava u odnosu na sve registrovane korisnike tog sistema.



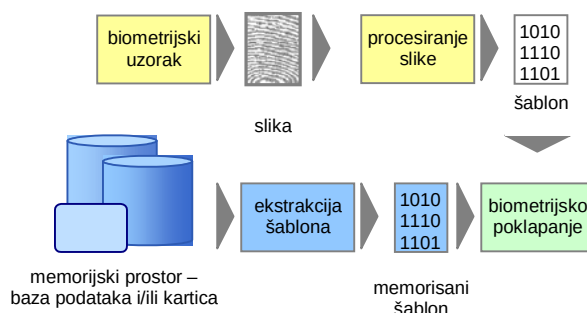
Slika 17 Upisivanje korisnika u biometrijski sistem

U osnovi svaki biometrijski sistem, bez obzira na kojoj tehnici je baziran, možemo podeliti na pet podsistema: prikupljanje podataka, procesiranje podataka, prenos podataka, skladištenje i pretraživanje podataka.

U ovom radu prikazana je metoda za prikupljanje podataka.

Prenos, skladištenje i pretraživanje/poređenje obavlja se nad šablonom (*template*). Svaka biometrijski zasnovan sistem prilikom verifikacije/identifikacije prolazi kroz četiri koraka:

- skeniranje (*snimanje*) uzorka,
- izdvajanje karakteristika (*pravljenje šablona*),
- upoređivanje šablona i
- nalaženje odgovarajućeg šablona, *slika 18*.



Slika 18 Verifikacija / identifikacija na osnovu biometrijskih podataka

Šablon je matematički obrađena i kodirana digitalna informacija zasnovana na izmerenim biometrijskim osobinama. Svaki šablon je jedinstven, ali se iz šablona ne može rekonstruisati polazna biometrijska informacija. Da bi se obezbedio pouzdan šablon, prilikom upisa korisnika u sistem uzima se više uzoraka iste biometrike, obično tri. Šablonu se pridružuje neki identifikator i onda se zajedno skladište. U zavisnosti od namene šablon može da se skladišti na samom uređaju za uzimanje podataka, u centralnoj bazi podataka, na čip (*smart*) karticama ili na nekom obeležju (*token*). Osnovni ciljevi svakog, pa i biometrijski zasnovanog sistema za verifikaciju su:

- da zabrani pristup svakoj osobi koja nema prava na pristup
- da obezbedi pristup svakoj osobi koja na to ima pravo

Sa stanovišta identifikacije neophodno je da sistem obezbedi pouzdano i jednoznačno pronalaženje osobe. U tom smislu razlikujemo i dve statističke veličine važne za delotvornost sistema:

- učestanost pogrešnih prihvatanja FAR^{16} - učestanost sa kojom sistem prihvata uljeza, i
- učestanost pogrešnih odbijanja FRR^{17} - učestanost sa kojom sistem odbacuje validnog korisnika.

Ove dve vrednosti zavise od primenjene biometrijske tehnike, uređaja koji se koriste za prikupljanje podataka, softverske obrade i načina skladištenja podataka.

¹⁶ FAR - False Accept Rate

¹⁷ FRR - False Reject Rate

3.3 BIOMETRIJSKE METODE

Biometrika kao tehnika identifikacije poznata je već od davnina. Stari Egipćani vršili su različita merenja tela osoba da bi ih identifikovali, u Vavilonu otisak prsta na glinenoj pločici korišćen je za poslovne transakcije, u staroj Kini stavljali su otisak palca na glinene pečate. U 14. veku u Persiji različita papirna državna dokumenta imala su na sebi i otisak prsta, a još tada je jedan državni lekar otkrio da ne postoje dva identična otiska. U novije vreme, Alphonse Bertillon (1870, Francuska) izmislio je sistem (*Bertillon sistem*) koji se bazira na analizi otisaka prstiju za identifikovanje kriminalaca. Francis Galton je među prvima razvio sistem za prepoznavanje na osnovu profila lica.

Veliki napredak napravljen je 60-tih i 70-tih godina prošlog veka, kada je za potrebe FBI razvijen sistem za automatsku identifikaciju pomoću otisaka prstiju - AFIS¹⁸. Danas razlikujemo dve osnovne klase biometrijskih tehnika: fiziološka tehnika (*Physiological-based techniques*) koja meri fiziološke karakteristike osobe, i tehnika koja se bazira na analizi ponašanja osobe (*Behavior-based techniques*).

Najpoznatije fiziološke tehnike (*Physiological - based techniques*) zasnivaju se na analizi otisaka prstiju, otisaka dlanova i na analizi lica. Ostale fiziološke tehnike su: analiza DNK, dužice oka, rožnjače oka, analiza geometrije dlanova, analiza struktura vena na šakama i druge. Tehnike na bazi ponašanja neke osobe (*Behavior-based techniques*) odnosno njenih osobina, jesu: analiza glasa, potpisa i načina kucanja po tastaturi.

¹⁸ AFIS - Automatic Fingerprint Identification System

3.4 METODE PREPOZNAVANJA NA OSNOVU FIZIOLOŠKIH OSOBINA

3.4.1 Metoda prepoznavanja pomoću otisaka prstiju

Prugaste šare i geometrija prstiju različiti su kod svake osobe, i ostaju nepromenjeni sa porastom tela. Identifikacija na osnovu otisaka prstiju je najstarija biometrijska tehnika koja se uspešno koristi za mnoge aplikacije. Automatski sistem za identifikaciju otisaka - AFIS igra značajnu ulogu u kriminologiji, kontroli pristupa, finansijskim transakcijama i u produkciji zvaničnih dokumenata (*vozačke dozvole, pasoši, lične karte*). To je on-line sistem u kome razlikujemo dva koraka:

- izdvajanje minucija i
- nalaženje odgovarajućeg uzorka u bazi otisaka.

Minucije su lokalne karakteristike brazda na prstima, javljaju se na krajevima brazda i pri račvanjima brazda. Minucije se prepoznaju (*izdvajaju*) i onda se mapira njihova relativna pozicija na prstu - koordinate x, y i ugao.



Slika 19 Otisak prsta i minucije

Da bi se smanjilo vreme pretraživanja uvedena je klasifikacija otisaka - indeksiranje, tako da se otisak poredi sa podskupom svih otisaka koji se nalaze u bazi i koji imaju odgovarajući indeks.

Sistem koji može da prepozna ove karakteristike je veoma kompleksan, ali i izuzetno precizan ukoliko se oslanja na nemodifikovane fizičke karakteristike. Ceo proces poređenja otiska sa bazom otisaka meri se sekundama, a tačnost je izuzetno velika.

U poređenju sa uređajima koji se koriste za ostale biometrijske metode uređaji za uzimanje otisaka spadaju među najjeftinije.

Postoje tri tehnike za skeniranje otisaka prstiju:

- optička,
- silikonska i
- ultrazvučna.

Optička metoda koristi rezoluciju od minimalno 500 tačaka po inču (*standard ANSI/NIST-ITL 1-2000*). Postoje i skeneri sa efektivnom rezolucijom do 1000 tačaka po inču. Silikonska tehnika zasniva se na manjoj površini skeniranja i preciznijoj slici; iako stiče sve veću popularnost mane su vreme potrebno za uzimanje otiska i prosleđivanje u sistem. Korišćenje ultrazvučnih signala za merenje karakterističnih razdaljina i dimenzija još uvek nije u širokoj upotrebi.

AFIS je jako pogodan za implementaciju u kartične sisteme kao što su magnetne kartice, smart kartice ili optičke kartice. Uvođenjem ove metode u postojeće sisteme za identifikaciju kao što su lične karte, vozačke dozvole, putne isprave, kreditne kartice i dr, u mnogome se povećava pouzdanost ovih sistema. Neki veliki proizvođači automobila koriste senzore za otiske prsta za identifikaciju vlasnika kao mehanizam sigurnosti. Pored sigurnosti može se povećati i komfor vozača, automatskim podešavanjem sedišta, retrovizora i temperature u kolima. Veliku primenu ova metoda nalazi u definisanju pristupa računaru i Internetu. Sve više proizvođača kompjuterske opreme ugrađuje senzore pomoću kojih se korisnici identifikuju i verifikuju. Zahvaljujući svojim prednostima kao što su jednostavnost i relativno niska cena u odnosu na druge biometričke metode, ova metoda je postala najrasprostranjenija biometrička metoda i pokriva 40% tržišta biometričkih tehnologija. U prilog korišćenju ovog verifikacionog postupka ide i raspoloženje korisnika. ANSI/NIST-ITL 1-2000 standard za informacione sisteme kojim se definiše format podataka za razmenu informacija o otiscima prstiju, licu osoba, uključivši i osobene znake - ožiljci, belezi i tetovaža, široko je podržan od strane proizvođača opreme koja se koristi sistemima na bazi biometrike.

Nedostatak ove tehnike je što se ne može koristiti kod osoba kojima nedostaju prsti, ili su prsti oštećeni i natečeni, a čitanje otisaka otežano je i kod starijih ljudi i, fizičkih radika i ljudi azijskog porekla. Nepravilno uzeti podaci od osobe mogu takođe dovesti do grešaka u identifikaciji i samim tim do neefikasnosti sistema.

3.4.2

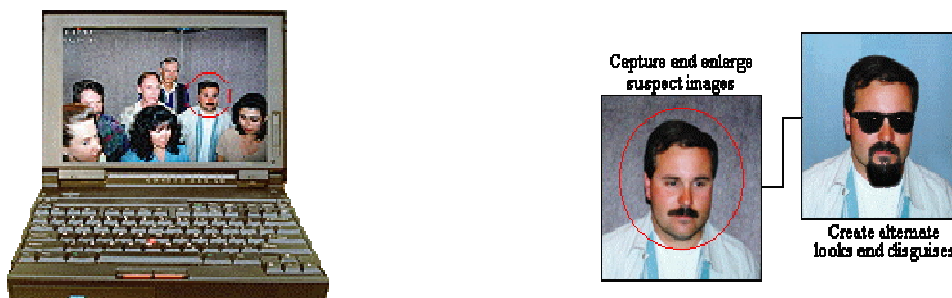
Prepoznavanje na osnovu analize lica

Ova tehnika zasniva se na analizi karakteristika lica koje su manje podložne promenama, kao što su: veličina nosa, oblik očiju, brada, obrve, usta, razmak između zenica i dr. Navedene osobine lica jedinstveno identifikuju neku osobu. Prepoznavanje na osnovu lica koristilo se ranije samo za vizuelnu verifikaciju osobe 1:1, ali razvijen je pouzdan sistem koji omogućava i identifikaciju. Danas su razvijene metode koje omogućavaju snimanje lica u kretanju, izdvajanje uzorka i identifikaciju. Vrlo bitna razlika u odnosu na ostale metode je što prepoznavanje lica može da se radi i pasivno - off-line skeniranje lica ljudi u gomili i naknadna pretraga u bazi. Ova karakteristika je konkretno omogućila značajno smanjenje ekscesa na fudbalskim utakmicama u Engleskoj, jer je sada moguća identifikacija i privođenje izgređenika i posle utakmica. U online režimu u nekim državama u SAD ovaj metod se primenjuje za prevenciju izdavanja višestrukih vozačkih dozvola i kartica za socijalno i zdravstveno osiguranje, dok ga neke zemlje već koriste prilikom glasanja za nacionalne izbore.

Kod metode prepoznavanja lica postoje dva različita pristupa:

- na osnovu lokalne analiza crta lica - LFA (Local Feature Analysis) i
- automatska obrada lica - AFP (Automatic Face Processing).

LFA je matematička metoda zasnovana na činjenici da se slika lica može predstaviti fiksnom grupom blokova koji zajedno čine šablon. Postoji više elemenata lica nego delova lica. LFA uzima u obzir desetine elemenata lica, uključivši podatke o delovima lica sa koga se te crte snimaju i relativne odnose između elemenata, i potom generiše šablon od blokova podataka. Kompleksna formula koja se koristi za mapiranje omogućava sistemu da se sa velikom tačnošću prilagodi brojnim promenama na licu, kao što su grimase, frizura, brada i brkovi, boja kože, naočare, (što je ilustrovano na slici 20), kao i promena osvetljenja i položaja lica, čak do 35°.

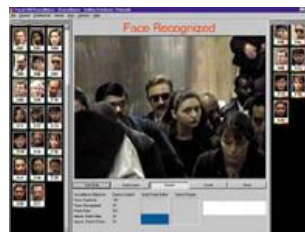


Slika 20 Prilagodljivost sistema kod LFA metode

Na slici 21 prikazana je identifikacija osobe snimljene u kretanju u gomili, na osnovu slike u mirovanju. Ova metoda je definisana standardom ANSI/NIST-ITL 1-2000.



uzorak slike osobe



prepoznavanje osobe na osnovu skeniranja u pokretu

Slika 21 LFA metoda

AFP se zasniva na merenjima rastojanja i odnosima rastojanja između lako prepoznatljivih delova lica, kao što su oči, nos i usta. Ovaj sistem je dosta uspešan kada se radi o zamagljenim i nedovoljno osvetljenim slikama, ali nema mogućnosti da se prilagođava promenama kao LFA.

Slike lica u oba slučaja zauzimaju između 150KB i 300KB, a šabloni koji se prave na osnovu slika veliki su do 3.5KB. Za sistem prepoznavanja na osnovu analize lica potrebna je vrlo kvalitetna video kartica, kamera i vrlo brz procesor za obradu podataka.

Verifikacija na osnovu analize slike lica se tradicionalno koristi za zvanična dokumenta, kao što su pasoši, vozačke dozvole i lične karte. Tehnologija koju smo opisali pruža dodatne mogućnosti za zaštitu građana i državnih institucija od zloupotreba i identifikaciju prestupnika. Međunarodna organizacija civilne avijacije ICAO je, kao i mnoge vlade širom sveta, takođe izabrala ovu biometrijsku tehnologiju za primenu u izdavanju pasoša.

3.4.3

Prepoznavanje na osnovu analize dužice oka

Prepoznavanje na osnovu analize dužice oka i prepoznavanje na osnovu analize mrežnjače oka dve su osnovne optičke metode. Oftalmolozi su od početka predlagali da dužica oka može biti iskorišćena kao neka vrsta optičkog otiska za identifikaciju ljudi. Njihov predlog bio je baziran na osnovu kliničkih rezultata koji pokazuju da je svaka dužica jedinstvena i nepromenljiva, čak postoji razlika između dužica levog i desnog oka iste osobe.



Slika 22 Struktura oka

Dužica se sastoji od mreže povezanih isprepletenih lanaca proteinskih vlakana, naboranih žljebova, krugova i boja - ukupno 266 različitih parametara.

Dužica poseduje neke osobine koje je čine vrlo pogodnom za korišćenje u automatskim identifikacionim sistemima:

- zaštićena je od spoljne sredine, vidljiva i sa rastojanja
- nemoguće je bez rizika po vid hirurškom intervencijom izmeniti dužicu
- fiziološki reaguje na svetlost što omogućava proveru prirodnosti
- slika dužice uzima se bez kontakta osobe i čitača (*skenera*), a može se lako uzeti i sa rastojanja.

Čitanje podataka obavlja se tako što se osoba postavlja na 30-tak cm ispred crno-bele kamere i gleda u uređaj za skeniranje. Kao i kod ostalih sistema, na osnovu skenirane slike i odgovarajućeg algoritma dolazi se do šablona, veličine 512 bajtova do 1000 bajtova, koji se zatim upoređuje ili sa bazom podataka - šablona, ili sa uzorkom koji se nalazi na nekom dokumentu. Razvijeni su i efikasni algoritmi koji iz video zapisa osobe u pokretu izdvajaju pouzdan opis dužice, generišu kompaktni kôd dužice i sa statistički velikom pouzdanošću ustanovljavaju identitet osobe. Ovaj sistem pouzdan je i u identifikacionom modu rada, i primenjiv na različite etničke grupe.

3.4.4

Identifikacija na osnovu senke

Špijunski sateliti uskoro će moći iz svemira da identifikuju osobu posmatrajući njenu senku. Sateliti će koristiti kompjuterski program koji prati pokrete senki na zemlji, a potom identifikuje vlasnika senke po načinu na koji hoda.

Ova tehnika, nazvana analiza hoda, oslanja se na činjenicu da način hoda teško može da se maskira.

Ova tehnologija mogla bi da se koristi za praćenje kriminalaca i osumnjičenih terorista uz upotrebu satelita ili špijunskih aviona.

Međutim, ova tehnika, koju je razvila NASA, potpuno je beskorisna kada nema sunca. Iako je došlo do velikog napretka u oblasti satelitskih snimaka i tehnologije u poslednjih nekoliko godina, još je nemoguće nekoga identifikovati na osnovu fotografija snimljenih iz svemira. Slike snimljene iz aviona koji leti na velikoj visini pokazuju samo teme glave.

Prema mišljenju dr Edrijena Stoike iz NASE, satelitski videosnimak mogao bi da da dovoljno podataka da se utvrdi identitet osumnjičenog ukoliko se način njegovog hoda nalazi u datoteci.

Prilikom identifikacije osoba, mogle bi se koristiti manje razlike u hodu, uključujući dužinu stopala, brzinu hoda, kretanje kukova i ugao između kolena, zgloba i kuka.

Dr Stoika je napravio kompjuterski softver koji prati i prepoznaje senke osoba na videozapisu snimljenom iz vazduha. On izdvaja pokretne senke i, uz upotrebu podataka o položaju Sunca i ugla kamere, koriguje senke ukoliko su skraćene ili izdužene.

Na testiranju videosnimka sa šestog sprata zgrade, njegov softver snimio je senke ljudi i izdvojio informacije koje bi se mogle upotrebiti radi identifikacije određene osobe. Ova tehnika je još u početnoj fazi i moglo bi proći još mnogo godina dok ne počne da se upotrebljava u vojne svrhe, u policiji i tajnim službama. Ona, ipak, ima i moguće nedostatke. Dok satelit koji vrši analizu načina hoda može biti koristan u zemljama kao što su Pakistan ili Irak, to neće biti uvek moguće u gradu kao što je, na primer, Mančester, iznad kojeg je tokom većeg dela godine nebo sivo i oblačno.

Stručnjak za fotografije snimljene iz svemira, Bupendra Jasani sa Kraljevskog koledža u Londonu, kaže da sateliti čije su kamere usmerene ka Zemlji jednostavno nemaju dovoljnu rezoluciju.

Kao i sateliti koji kruže orbitom, i špijunski avion poput RAF „nimroda“ mogu kružiti na velikim visinama posmatrajući snajperiste na zemlji, bilo po danu, bilo noću, uz upotrebu termalnih kamera visoke definicije.

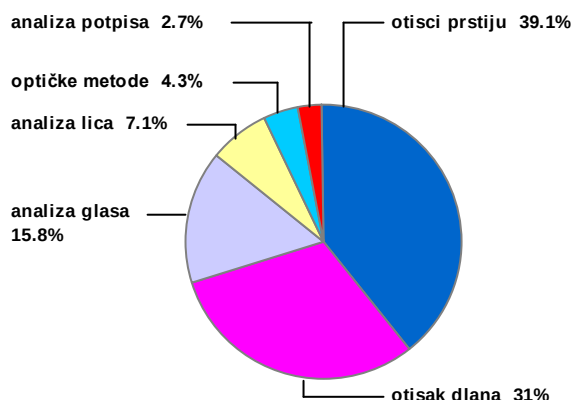


Slika 23 Identifikacija na osnovu senke

3.5

OBLASTI PRIMENE BIOMETRIJSKIH METODA

Mnogobrojne su oblasti primene biometrijskih metoda, samostalno ili u kombinaciji sa još nekom metodom, kao što su npr. zaštićene identifikacione kartice (*smart kartica ili barkod*). U nekim sistemima koriste se i kombinacije više biometrijskih metoda, tako da se maksimalno koriste dobre strane svake tehnike. Na primer, kombinovanjem analize lica sa otiscima prstiju i dlana dobija se vrlo sofisticiran i pouzdan mehanizam za identifikaciju. Zastupljenost biometrijskih metoda na svetskom tržištu ilustrovana je na slici 24 (podaci iz 2000. godine).



Slika 24 Zastupljenost biometrijskih metoda na tržištu

Biometrika se primenjuje za sledeće aplikacije:

- vladine institucije - pasoš, lična ID kartica, vozačka dozvola, saobraćajna dozvola, dozvola za nošenje oružja
- socijalna zaštita - kartica za nezaposlenog, penzionerska kartica
- zdravstvena zaštita - zdravstvena kartica, ID kartica za pacijenta, ID kartica za zdravstvenog radnika
- finansijske transakcije - bankovna kartica, bankomat kartica, čekovna kartica, elektronsko poslovanje, sefovi, kartice za kupovinu
- prevoz i putovanja - bording karta za avion, bezbednost na aerodromima i u hotelima
- bezbednost - kontrola pristupa i verifikacija identiteta i kontrola prisustva osobe: za ustanove, organizacije, industrijska postrojenja, fabrike, objekte posebne namene, računarske mreže i baze podataka itd.
- zatvori - ID kartica zatvorenika, ID kartica posetioca
- javna bezbednost - identifikacija kriminalaca
- obrazovanje - ID kartica za studentski dom
- oružje - tzv. „bezbedno“ lično oružje koje može samo jedna osoba da aktivira

3.6 BIOMETRIKA I SMART KARTICE

Smatra se da je kombinacija biometrike i smart kartica najpogodnija i u isto vreme najsigurnija mogućnost za realizovanje sistema za identifikaciju lica. U svetu je opšti trend da se ID kartice unapređuju dodavanjem biometričkih karakteristika, prvenstveno u cilju borbe protiv terorizma i organizovanog kriminala. Ovo može biti realizovano i sa klasičnim štampanim identifikacionim karticama i sa čip karticama, a identifikacija može biti anonimna, decentralizovana ili podržana od sistema koji u pozadini ima veliku banku podataka.

Kao i kod identifikacionih kartica koje su sada u upotrebi, biometrički podaci koji se uzimaju od osobe mogu biti uništeni odmah posle smeštanja na neku ID karticu. Ovo znači da bi se oni nalazili jedino na kartici i bili bi pod isključivom kontrolom vlasnika kartice. Jedan od načina smeštanja biometričkih podataka na ID kartice je integracija, na klasičnim papirnim karticama, digitalnog vodenog žiga na fotografije ili biometričkih podataka na hologram. Na ovaj način identifikacione kartice će izgledati kao i ranije. Međunarodna organizacija za uspostavljanje standarda za ID kartice koje su mašinski čitljive, ICAO, prihvatiće i ID kartice na bazi smart kartica. Osim dobijanja ICAO odobrenja, čip kartice, koje se odnose na ID kartice, imaju tu prednost da mogu da budu jako raznovrsne i prilagodljive. Podaci sa smart kartica mogu se koristiti u različitim uređajima i mrežama.

Biometrijski podaci mogu biti smešteni na smart karticu, u lokalni čitač ili u centralnu bazu podataka. Kod ID sistema baziranih na smart karticama biometrika i druge personalne informacije nalaze se na kartici, uvek uz vlasnika kartice. Kod ovakvih sistema moguća je offline provera, što značajno smanjuje vreme potrebno za proveru identiteta neke osobe.

Da bi skladištila odgovarajuće biometrijske podatke smart kartica mora imati dovoljno memorije. Kod nekih aplikacija biometrika i personalne informacije mogu biti smeštene u čitač. Ove aplikacije zahtevaju da se smart kartice koriste sa pojedinačnim čitačem, ili ako postoji nekoliko pristupnih tačaka, baza biometričkih podataka i čitač moraju biti umreženi. Centralna baza podataka, kao skladište za biometričke podatke, mora imati visok nivo zaštite, a za slučaj da upravlja mnogostrukim tipovima čitača, koji koriste iste biometričke podatke, oni moraju imati različite algoritme.

Korišćenje smart kartica značajno povećava pouzdanost kod biometričkih ID sistema. Smart kartice skladište i obezbeđuju personalne informacije, tako da, svakom korisniku nude jedinstvenu zaštitu i prenosivu, ličnu bazu podataka, razdvajajući njegove informacije od informacija drugih korisnika. Vlasnik kartice fizički poseduje privatne informacije. Ovo unapređuje poverenje između njega i sistema, tako što korisnik sada učestvuje u odluci ko može da koristi njegove lične podatke za verifikaciju identiteta i odgovoran je u zaštiti tih podataka. Dodavanjem biometrike, smart kartice obezbeđuju jedinstvenu vezu između vlasnika kartice i privatnih podataka na kartici, identifikujući onoga ko poseduje karticu kao pravog vlasnika kartice. Biometrika se ne može pozajmiti, izgubiti ili ukrasti kao PIN ili lozinka, što poboljšava verifikaciju identiteta neke osobe.

U ID sistemima na bazi smart kartica, kartica nije samo skladište podataka, već i inteligentni čuvar personalnih informacija vlasnika kartice. Ove kartice daju vlasniku kontrolu ko može da pristupi njegovim podacima. A biometrika dodatno osigurava da samo pravi vlasnik može da dozvoli pristup personalnim informacijama.

Kod smart kartica sa biometrikom, može se digitalno potpisati biometrika u procesu upisivanja na karticu i može se proveravati poređenjem sa uzetom biometrikom od strane čitača, svaki put kada se kartica koristi. Biometričke informacije, kao i druge personalne informacije koje se nalaze na kartici mogu biti enkriptovane, kako bi se ti podaci što bolje zaštitili od spoljnih napada. Upoređivanje biometričkih podataka sa kartice i onih trenutno uzetih preko čitača, obavlja se tako da biometrički podaci sa kartice nikad ne napuštaju karticu, pa su tako zaštićeni od promena tokom prenosa. Na ovaj način mogu efikasno i da se zaštite ostale informacije smeštene na kartici, kao što su ključevi za enkriptovanje e-mail-a ili podaci za digitalni potpis. Tako na primer, ako je potreban digitalni potpis za potvrđivanje neke operacije, biometrički podatak osigurava da potpis vlasnika kartice ne može biti zloupotrebljen od nekog drugog. Smart kartice imaju dovoljno memorije da smeste velike količine podataka, koje mogu da se dodaju, uključujući i programe, jednu ili više biometrika, mnogostruke kriptografske ključeve za ograničavanje pristupa podacima, kako bi se osigurali od promena, brisanja ili dodavanja.

3.7 ZAKLJUČAK

Ovde smo razmatrali biometrijske metode, zasnovane na analizi fizioloških osobina i na analizi ponašanja osobe. Biometrika je siguran i pouzdan način za identifikaciju i verifikaciju ljudi i ima velike prednosti u odnosu na tradicionalne metode. Uvođenje biometrike u informacione sisteme višestruko će poboljšati rad i usluge:

- verifikacija i identifikacija zasnivaju se na podacima koje osoba uvek nosi na sobom: 50% svih poziva koji stižu službama za pružanje usluga korisnicima odnose se na zaboravljene lozinke i PIN kodove sigurnost i pouzdanost: uzorci su jedinstveni za svaku osobu, šabloni koji se prave na osnovu uzoraka su takođe jedinstveni ali se ne može reverzibilnim procesom dobiti originalna slika uzorka, što dodatno obezbeđuje tajnost podataka onemogućava krađu identiteta: kombinovanjem više biometrijskih šablona, ili neke biometrijske metode i identifikacione kartice (barkod, smart kartica, token), dobija se ključ koji se praktično ne može falsifikovati, ili ukrasti i upotrebiti jer nije moguća naknadna izmena kodova i podataka
- obezbeđuje se tajnost ličnih podataka: privatnost osobe nije ugrožena, naprotiv identitet osobe je dodatno osiguran i zaštićen od krađa i zloupotreba bezbednost: povećava nivo bezbednosti i zaštite.

3.7.1 Da li nam je biometrika potrebna?

Da, i to što pre, naročito u informacionim sistemima državnih organa i institucija. Imajući u vidu preporuke i standarde međunarodnih tela kao što su ICAO i ANSI/NIST, kao i praksu i iskustva koje imaju vlade vodećih industrijskih i tehnoloških zemalja.

Novi funkcionalni sistem na bazi multimedijalne tehnologije obezbediće dosad najveći nivo pravne, imovinske i lične zaštite i sigurnosti građana. Ovakav sistem nudi sigurno, brzo i efikasno utvrđivanje identiteta lica, kao i zaštitu sigurnosti dokumenata i privatnosti podataka građana. Sistem će omogućiti jednostavniji, pouzdaniji i kvalitetniji rad sa građanstvom, uz puno poštovanje domaćih i međunarodnih normi i deklaracija o zaštiti ličnih podataka u sistemima automatske obrade.

Sastavni deo novog funkcionalnog sistema koji na bazi multimedijalne tehnologije obezbeđuju zaštitu, arhiviranje, razmenu i pretraživanje dokumenata i podataka biće automatsko prepoznavanje otisaka prstiju i dlanova i fotografija lica. Kombinacija ovih metoda daje najbolje rezultate, po pitanju tačnosti i pouzdanosti, jednostavnosti i funkcionalnosti primene, i značajnoj činjenici da svaka osoba u populaciji može biti registrovana. Sistem MUP-a Republike Srbije koristiće opremu i softver za obradu, transfer i skladištenje podataka koji su svi u skladu sa ICAO i ANSI/NIST standardima, što je vrlo važan preduslov za integraciju naše zemlje u međunarodnu zajednicu.

Postoje različite biometrijske standardizacione inicijative koje se tiču kako biometrijskih podataka na samoj kartici, tako i razmene takvih podataka.

BioAPI¹⁹ standard pruža jedan visokokvalitetni model biometrijske autentikacije i to nezavisno od primenjene tehnologije. On pokriva kako funkcije za upisivanje biometrijskih podataka na karticu i u bazu, verifikaciju i identifikaciju, tako i standarde za interfejs za bazu biometrijskih podataka.

CBEFF²⁰ je biometrijski standard koji se tiče razmene i međunarodne primenljivosti biometrijskih podataka.

¹⁹ BioAPI - Biometric Application Program Interface

²⁰ CBEFF - Common Biometric Exchange File Format

GLAVA IV

4 ELEKTRONSKI IDENTITET GRAĐANA I MOGUĆNOSTI NJEGOVE PRIMENE

4.1 UVOD

Zloupotreba identiteta, u obliku krađe identiteta ili višestrukog identiteta, je krivično delo koje je sve zastupljenije danas u svetu. Takođe, zloupotreba elektronskog identiteta je jedna od najzastupljenijih vrsta kompjuterskog kriminala.

Prema izveštaju UK iz 2002.godine, za samo pola godine zloupotreba identiteta je prouzrokovala oko 2 milijarde evra troškova, što u poređenju sa ukupnim godišnjim troškovima izazvanim svim krađama (*19,8 milijarde evra*) nije mali iznos. U Americi, krađa identiteta svake godine uzrokuje 700.000 žrtava. Svaka od njih potroši prosečno 808 dolara za pokriće troškova izazvanih zloupotrebom vlastitih dokumenata, i, u proseku, 175 časova za obaveštavanje kreditnih biroa, poništavanje kreditnih kartica, pregovore sa kreditorima radi vraćanja poverenja.

Ova vrsta krivičnog dela je često u vezi sa ostalim vrstama kriminala, kao što su pranje novca, trgovina ljudima i lažno predstavljanje.

Porast krivičnih dela zloupotrebe identiteta objašnjava se slabošću u postupku izdavanja identifikacionih dokumenata i postupku provere identiteta pojedinaca zasnovanom na tako izdatom dokumentu. Slabost u sistemu utvrđivanja i provere identiteta osoba uopšte, a posebno na graničnim prelazima i aerodromima može jednu zemlju učiniti potencijalno atraktivnom metom terorističkih grupa.

Upravo strah od terorističkih napada uticao je na pojavu trenda uvođenja obaveznih identifikacionih dokumenata, kao i putnih isprava sa biometrijskim podacima vlasnika. Takav izbor je logičan, jer se biometrijski identitet ne može falsifikovati ili kopirati.

Nova napredna tehnologija sigurno može da pomogne u uspostavljanju jednog pouzdanog sistema identifikacije lica i zaštite identifikacionih dokumenata koji će, na prvom mestu, povećati njihovu upotrebljivost i pouzdanost, te da će doprineti smanjenju zloupotreba.

SMART kartica sa biometrijskim podacima vlasnika (*digitaina fotografija obavezno i opcionalno otisak prsta, analiza dužice oka ili DNK analiza*) i infrastrukturu javnih ključeva - PKI, koja štiti podatke u čipu kartice i elektronskim transakcijama (*omogućava pouzdanu autentikaciju, tajnost, integritet i raspoloživost podataka*), nameću se kao prirodno rešenje za pouzdan identifikacioni dokument kako u realnom tako i u svetu digitaine komunikacije.

Glavni ciljevi savremenih identifikacionih sistema građana su:

- efikasna kontrola (*granica, ulica, aerodroma,...*)
- pouzdano legitimisanje građana
- sigurna identifikacija u bankarskim i drugim administrativnim poslovima.

4.2 ELEKTRONSKI IDENTITET LIČNOSTI

Identitet (lat. *IDEM*, isto; nlat. *IDENTITAS*, istovetnost) predstavlja osnovnu određenost stvari, događaja i ljudi koja omogućava imenovanje, poznavanje i prepoznavanje.

Identitet ličnosti predstavlja jedinstvenu kombinaciju karakteristika koje se odnose na svako fizičko lice, u skladu sa nacionalnim ili međunarodnim zakonima, onako kako je odgovarajuće, dozvoljava njegovu ili njenu individualizaciju od strane nadležnih državnih organa, tj. obuhvata zbir opštih i osobenih znakova karakterističnih za jednu osobu kojima se ona razlikuje od ostalih osoba i po kojima se sigurno može prepoznati (*identifikovati*), kao što su ime, prezime, datum i mesto rođenja, pol, fizičke karakteristike, itd.

Identitet osobe obuhvata sledeće elemente:

- **osobeni identitet** je zasnovan na podacima koje svaka osoba stiče po rođenju (*ime, prezime, datum i mesto rođenja, kao i podaci o roditeljima*)
- **biografski identitet** je identitet u formi zvaničnih dokumenata i uverenja i nastaje međusobnim uticajem pojedinca i različitih organizacija i udruženja tokom života; škola, opštinskih organa, banaka, penzionog fonda... (*lekarski kartoni, školske diplome, radna knjižica i ostala dokumenta...*)
- **biometrijski identitet** je identitet određen jedinstvenim fizičkim osobenostima i predstavlja pouzdan način za proveru i potvrdu identiteta osobe (*otisak prsta, dlana, analiza lica, slika dužice oka, DNK analiza...*)

Sa druge strane možemo sagledati fizički identitet (*biometrijske karakteristike, stečeni identifikacioni podaci u realnom svetu*) odnosno elektronski identitet (*logički, digitalni identitet u elektronskoj komunikaciji*) osobe.

Provera identiteta se najčešće obavlja upotrebom dokumenta sa fotografijom (*identifikacioni dokumenti, putne isprave ili specifični dokumenti*).

Prema definiciji TER-S-IT (*Grupe specijalista za identifikaciona dokumenta i terorizam pri Savetu Evrope*):

- Identifikacioni dokument znači svaki dokument koji izdaju nadležni državni organi u skladu sa nacionalnim zakonom u cilju potvrde identiteta nosioca dokumenta.
- Putna isprava znači svaki zvaničan dokument koji izdaju državne ili nadležne organizacije, koji koristi nosilac dokumenta radi međunarodnih putovanja i koji sadrži obavezne vizuelne podatke i uopšteno sliku nosioca.

Sa aspekta pouzdanosti identiteta, tradicionalne metode utvrđivanja identiteta, nisu dovoljno pouzdane da spreče zloupotrebe. Razlog je slabost u postupku izdavanja identifikacionih dokumenata i u postupku provere identiteta lica zasnovanom na tako izdatom dokumentu. To isto čini jednu zemlju potencijalno atraktivnom metom terorističkih grupa i mreža.

Moderna tehnologija uključivanjem mašinski čitljivih biometrijskih podataka vlasnika i rešenja zaštite podataka putem infrastrukture javnih ključeva u savremena (*elektronska*)

identifikaciona dokumenta, uz postavljanje takvih dokumenata integralnim delom kompleksnog IT sistema, omogućava uspostavljanje pouzdanog sistema identifikacije lica i zaštite identifikacionih dokumenata u realnom i digitalnom svetu koji će, pre svega, povećati njihovu upotrebljivost i pouzdanost, i time doprineti smanjenju zloupotreba.

Uključivanjem biometrijskih podataka (*otisaka prstiju i karakteristika lica*) u aktivnosti vezane za kontrolu lica dobija se automatski odgovor na tri kjučna pitanja:

- **verifikacija:** „Da li sam ja onaj ko kažem da sam?“
- **identifikacija:** „Ko sam ja?“
- **pretraga kroz hot bazu:** „Da li me tražite?“

Uključivanjem infrastrukture javnih ključeva i digitainih sertifikata omogućava se pouzdana verifikacija podataka i garantuju njihova poverljivost, integritet i neporecivost.

4.3 ELEKTRONSKI IDENTIFIKACIONI DOKUMENTI

Primena smart kartica kao identifikacionih dokumenata predstavlja najrasprostranjeniju tehnologiju za proveru i utvrđivanje identiteta u svetu. Uvođenje elektronskih ličnih dokumenata, na prvom mestu, ima za cilj ustanovljenje pouzdanog i sigurnog dokumenta za potvrdu identiteta građana i efikasan rad državne administracije, pružanje novih elektronskih usluga građanima i sprečavanje zloupotreba i falsifikata.

Mnogobrojne su prednosti u poređenju sa drugim rešenjima, pre svega papirnim identifikacionim dokumentom:

- Pored estetskih, takva dokumenta su trajnija i izdržljivija na fizička oštećenja
- Ugrađeni čip je pogodan za smeštanje velikog broja podataka, kao i za smeštanje biometrijskih podataka vlasnika. Ugrađeni, veoma precizni, zaštitni mehanizmi sprečavaju nedozvojene pristupe i obrade podataka
- Ugrađeni softverski i hardverski zaštitni mehanizmi u veoma visokom stepenu doprinose zaštiti od prevara, krađa, falsifikata
- Ugrađena poluprovodnička tehnologija omogućava automatsko poništavanje eID kartice po isteku roka važnosti dokumenta, odnosno blokiranje kartice ili brisanje memorije po detekciji nedozvoljenih pristupa podacima
- Pojednostavljen postupak u slučaju gubitka, krađe ili kvara.
- Različita primena (*kombinovanje eID sa nekim drugim dokumentom, npr. vozačkom dozvolom, zdravstvenom knjižicom, službenom karticom ili korišćenje drugih elektronskih servisa*). U Finskoj je eID ujedno i bankarska kartica.
- Brza i pouzdana identifikacija i autentikacija vlasnika u elektronskoj komunikaciji
- Veoma brza provera identiteta jer vlasnik eID kartice svoje biometrijske podatke nosi „sa sobom“, na kartici.

Ovlašćeno lice pomoću čitača SMART kartice vrši poređenje biometrijskih podataka upisanih na čipu (*na primer otiska prsta*) i onih uzetih na licu mesta (*otiska uzetog pomoću skenera otisaka*).

Pojednostavljena kontrola lica na aerodromima i graničnim prelazima, što sve doprinosi povećanju nivoa bezbednosti i sigurnosti građana. Nije bitno ko prelazi granicu (*imenom i prezimenom*), već da je osoba zaista ona čiji identitet dokument potvrđuje. Akcenat je na pouzdanom postupku izdavanja dokumenta.

Primena elektronskog identifikacionog dokumenta mora da osigura:

- Pouzdanu verifikaciju korisnika, aplikacija, transakcija, odnosno da osigura da samo ovlašćena lica pristupaju važnim podacima ili da vrše obradu podataka
- tajnost, odnosno poverljivost podataka odnosno da lični i poverljivi podaci budu zaštićeni od neovlašćenih pristupa
- integritet podataka odnosno da nije moguće bilo kakvo menjanje podataka od strane neovlašćenih lica
- raspoloživost podataka odnosno da su oni dostupni ovlašćenom licu ili aplikaciji kad god je to potrebno

Svakom od ovih zahteva udovoljava se različitim sigurnosnim merama - pouzdana verifikacija se postiže korišćenjem lozinke, PIN-a ili biometrike ili njihovom kombinacijom,

dok se tajnost podataka može osigurati na primer enkripcijom podataka ili sigurnim smeštanjem podataka na karticu.

Složeniji informaciono telekomunikacioni sistem (*slučaj eID*) mora imati optimalnu kombinaciju različitih sistema zaštite.

Za sada, najnapredniji sistem zaštite pruža kombinacija smart kartica, biometrijskih podataka vlasnika kartice i infrastrukture javnih ključeva.

Odgovornost za čuvanje eID je na vlasniku dokumenta, naime, vlasnik je obavezan da čuva eID i PIN broj prema uslovima određenim ugovorom između vlasnika dokumenta i izdavaoca ličnog identifikacionog dokumenta radi sprečavanja eventuačnih zloupotreba.

U slučaju dodavanja drugih aplikacija na eID, upisivanje dodatnih aplikacija u slobodnoj memoriji čipa mora biti zaštićeno PIN-om i/ili biometrikom pri čemu je preporučljivo da svaka aplikacija ima svoj poseban PIN. Takođe smeštanje aplikacija i poništavanje njihove upotrebe mora biti pravno regulisano između vlasnika kartice i pružaoca elektronske usluge.

Rok važnosti izdatog eID i pripadajućih sertifikata propisuje država izdavač (5-10 godina). Produženje važnosti kartice i sertifikata treba da bude pravno regulisano i da se vrši po odgovarajućoj i sigurnoj proceduri, kao i njihovo izdavanje.

Poništavanje eID i pripadajućih sertifikata vrši se automatski po isteku roka važnosti. U slučaju gubitka, krađe, ili kvara elektronskog dokumenta, postupak poništavanja kartice je na zahtev vlasnika i podrazumeva poništavanje svih izdatih sertifikata. Samu karticu nije potrebno poništavati. Korišćenje elektronskog dokumenta i njegovih sertifikata u elektronskoj komunikaciji se ukida unošenjem sertifikata na listu ukinutih sertifikata. CA treba da pruži pouzdan i lako dostupan, on-line, servis za blagovremenu proveru statusa i suspenziju sertifikata, koji radi u realnom vremenu.

4.4 Elektronski identifikacioni dokumenti u Srbiji

Primarni identifikacioni dokument je lična karta - jedini i osnovni dokument za potvrdu identiteta vlasnika dokumenta.

Sekundarni identifikacioni dokumenti su: vozačka dozvola, saobraćajna dozvola, dozvola za nošenje oružja i putna isprava (*e-passport*) i služe za potvrdu podataka koji su u njima navedeni, a njihovo korišćenje uključuje i korišćenje primarnog identifikacionog dokumenta. Tehnološki uslov za izdavanje bilo kog sekundarnog identifikacionog dokumenta je postojanje primarnog. Putna isprava se može smatrati primarnim ID kada se koristi u inostranstvu, dok se za korišćenje u zemlji ona smatra sekundarnim ID.

Pored primarnih i sekundarnih identifikacionih dokumenata moguća je primena i ostalih dokumenata kao što su identifikacione kartice za posebne namene, zdravstvena legitimacija...

4.4.1 Primena

Elektronska dokumenta i elektronski identitet imaju značajnu ulogu u oblasti državne uprave (*elektronska identifikaciona dokumenta, putne isprave, vozačke dozvole, saobraćajne dozvole, dozvole za nošenje oružja, kartice za socijalnu zaštitu, socijalnu pomoć i penzije, kartice za zdravstveno osiguranje, e-government...*), u komercijalnim primenama (*bankarstvo - kreditne i debitne kartice, elektronsko bankarstvo, e-business, e-commerce, mobilna komunikacija - SIM kartice, transport, TV pretplata, članske karte...*) i u širokom opsegu ličnih primena (*zaštita stanova, kola, mobilnih telefona...*).

U komercijalnoj i oblasti državne uprave informaciona šema za primenu elektronskih dokumenata može biti eksterno (*za korisnike komercijalnih usluga, odnosno građane*) ili interno dizajnirana (*službene kartice za zaposlene*).

U procesu potvrde identiteta uključivanje mašinskih i elektronskih provera omogućava mašinsko iščitavanje podataka i njihovo poređenje sa podacima smeštenim u HOT bazama, autentifikaciju zaštitnih elemenata dokumenta, verifikaciju biometrike na osnovnom nivou kontrole. Na srednjem nivou kontrole vrše se automatska analiza dokumenata tehničkim poređenjem sa referentnim standardima i višestruka biometrijska identifikacija, dok se na najvišem nivou kontrole vrše forenzičke analize prema manipulaciji IT funkcija i mašinski proverljivih zaštitnih elemenata.

U skladu sa savremenim tehnologijama integrisanim u izradu elektronskih identifikacionih dokumenata realizovane su i adekvatne tehnološke mogućnosti uređaja za validaciju elektronskih dokumenata.

Savremeni uređaji omogućavaju i sledeće funkcionalnosti:

- Mogućnost različitih načina skeniranja dokumenta (*realna, UV, IC svetlost*) radi provere zaštitnih elemenata



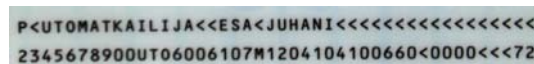
Slika 25 Skeniranje dokumenata osvetljenog različitim vrstama svetlosti

- Čitanje podataka smešteni na zaštićeni način u 2D barcod i njihovo dekodiranje



Slika 26 Prikaz dekodiranih podataka iz 2D barcoda

- Čitanje podataka sa OCRB (*pre svega za iščitavanje mašinski čitljive zone - MRZ koja postaje propisani standard na identifikacionim dokumentima*)



Slika 27 Zapis MRZ iščitán OCR-B-om

- Uzimanje otiska prsta alive na licu mesta od prisutne osobe
- Poređenje otiska prsta uzetog alive sa otiskom prsta na zaštićen način smeštenim u identifikacionom dokumentu (*u 2D barkodu ili čipu*)



Slika 28 Uzimanje alive otiska prsta i njegovo poređenje sa zapisom na dokumentu

- Čitanje elektronskih podataka iz kontaktnog i beskontaktnog čipa
- Poređenje podataka na različite načine iščitanih sa dokumenta

Savremeni uređaji za validaciju (*verifikacija i identifikacija*) mogu se koristiti kao periferali fiksnih radnih stanica ili mogu biti mobilne radne stanice. Mobilne radne stanice mogu raditi u on-line (*postavljanjem upita ka centralizovanim bazama podataka*) i/ili u off-line režimu. Za operativne potrebe neophodna je ažurnost tog fonda podataka pa se periodično vrši preuzimanje i sinhronizacija tih podataka sa sadržajem centralizovanih baza podataka.

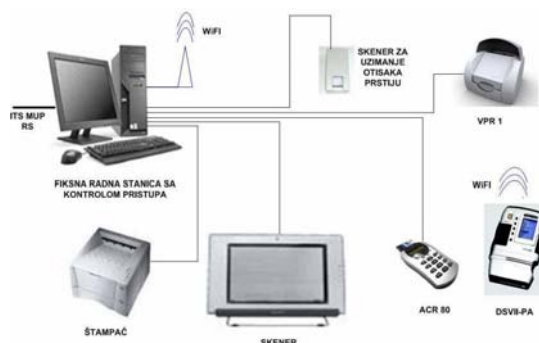
Zbog velikog značaja i kritičnosti kontrole prelaska državne granice fiksna radna stanica za kontrolu prelaska putnika na graničnim prelazima opremljena je kompletnim setom najsavremenijih uređaja za validaciju koji uključuje:

- Stacionarni uređaj za validaciju putnih isprava (*sa integrisanim skenerom površine putnih isprava i ID dokumenata, čitačem kontaktnih čipova*)
- Skener za uzimanje alive otisaka prstiju
- Stacionarni uređaj za validaciju elektronskih ID dokumenata u formi smart kartice
- Mobilni kombinovani uređaj za validaciju elektronskih ID dokumenata i putnih isprava, sa integrisanim Fingerprint modulom, čitačem kontaktnih i beskontaktnih smart kartica i skenerom 2D barkoda.

Za potrebe realizacije projekta ITS - IPS i servisa e-Police u okviru njega uočena je potreba za realizacijom fiksnih radnih stanica za akviziciju, validaciju i kontrolu prelazaka državne granice, mobilnih radnih stanica koje će se primenjivati na graničnim prelazima, u delokrugu aktivnosti saobraćajne policije, za regulisanje javnog reda i mira itd., kao i sistema fizičke kontrole pristupa zaštićenim oblastima (*Access control point*).



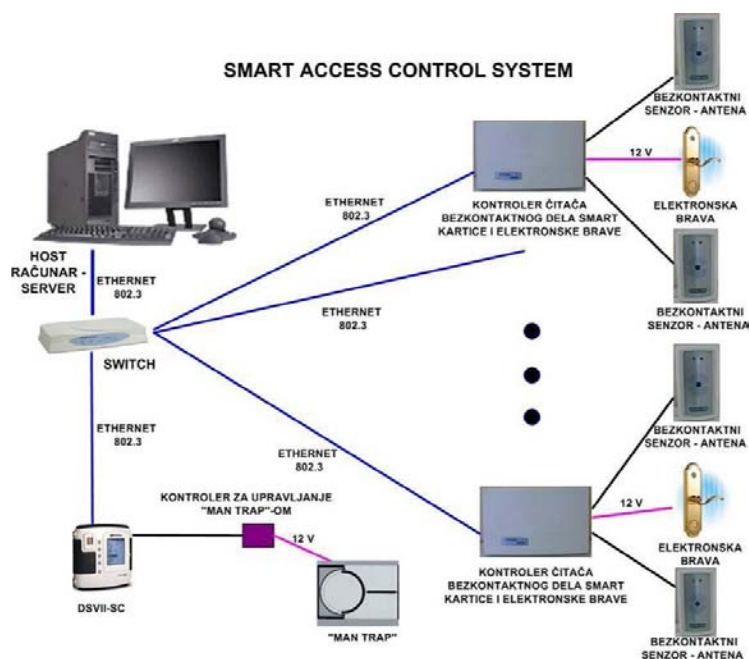
Slika 29 Primena u okviru e-Police



Slika 30 Radna stanica za kontrolu prelaska državne granice

Savremene tehnološke mogućnosti verifikacije i autorizacije osoba se primenjuju i u sistemima za fizičku kontrolu pristupa zaštićenim oblastima. To je zapravo integrisani sistem najsavremenijih uređaja i sistema aplikacija zasnovanih na proveri identiteta. Ovaj sistem je prikazan na slici 30. i ima sledeće glavne komponente:

- HOST računar sistema
- Čitač i pisac beskontaktnih RF-ID smart kartica
- Kombinovani čitač smart kartica (*kontaktnih i beskontaktnih*) sa biometrikom
- Elektronske barijere (*brave, rampe i magnetni kontakti*) za kontrolu fizičkog pristupa
- Kontroler čitača beskontaktnih smart kartica i elektronske brave sa dva beskontaktna senzora - antene i aplikacija na njemu
- Kontroler kombinovanog čitača smart kartica sa biometrikom
- Kontaktne smart kartice
- Beskontaktna RF-ID smart kartice
- Serverska aplikacija na HOST-u za administraciju i konfiguraciju sistema
- Serverska aplikacija na HOST-u za kontrolu pristupa oblastima (*servisira klijente - Kombinovane čitače smart kartica sa biometrikom*)
- Serverska aplikacija na HOST-u za kontrolu pristupa zonama i prostorijama unutar oblasti (*servisira klijente - Kontrolere čitača beskontaktnih smart kartica i elektronskih brava sa dve antene*)
- Aplikacija za personaiizaciju beskontaktnih RF-ID smart kartica
- Baza podataka lica kojima je omogućen pristup sa dodeljenim pravima pristupa određenim oblastima ili objektima
- Klijentska aplikacija na Kombinovanom čitaču smart kartica sa biometrikom



Slika 31 Fizička kontrola pristupa zaštićenim oblastima

4.5 Servis elektronske vlade (*e-vlada*)

Elektronska vlada (*e-vlada*), po konceptu i realizaciji, je servis koji omogućava građanima obavljanje različitih upravnih poslova (*državljanstvo, prijave i odjave boravišta, podnošenje zahteva organima državne uprave i praćenje realizacije, uvid u lične podatke, glasanje...*) elektronskim putem. Te poslove građani tradicionalno obavljaju na šalterima što, po pravilu, oduzima puno vremena kako njima samima tako i organima državne uprave.

Ovaj elektronski servis organima državne uprave skraćuje vreme obrade dokumenata, i predstavlja posebnu pogodnost za stanovništvo, jer se elektronske transakcije mogu obaviti nezavisno od radnog vremena datih organa i njihovog mesta.

Građani jednostavnim uključanjem na poznatu internet adresu servisa i autorizacijom eID, dolazi do željene usluge nezavisno od mesta gde se nalazi, i to brzo, jednostavno, efikasno. Ovaj elektronski servis može biti organizovan preko mreže elektronskih kioska instaliranih na javnim mestima.

Elektronska vlada, u suštini znači, da podaci „putuju“ umesto građana.

Razlikujemo sledeće nivoe razvijenosti elektronskih servisa organa državne uprave:

- **Početni nivo** e-vlade karakteriše postojanje zvaničnog WEB sajta na Internetu koji daje osnovne informacije o radu, budućim planovima...
- **Napredniji nivo** e-vlade uključuje više zvaničnih WEB sajtova, koji se često ažuriraju, kao i postojanje linkova i mogućnost kontakata elektronskom poštom.
- **Interaktivni nivo** e-vlade omogućava građanima korišćenje elektronskih formulara, kontakte sa službenim licima putem elektronske pošte, slanje komentara, primedbi, predloga i pretraživanje po određenim bazama podataka.
- **Transakcioni nivo** e-vlade omogućava građanima obavljanje određenih transakcija i korišćenje elektronskih usluga uz plaćanje određene naknade. To mogu biti usluge izdavanja izvoda iz matičnih knjiga, registracije vozila, usluge izdavanja putnih isprava i dr. Ovaj nivo usluga elektronske vlade podrazumeva korišćenje digitalnog potpisivanja, kao i neki od načina pouzdane provere elektronskog identiteta odnosno autentikacije (*PIN i lozinka, ili biometrijske metode*).
- **Integralni nivo** e-vlade predstavlja najviši nivo elektronskih servisa i omogućava potpunu integraciju vladinih elektronskih usluga sa ostalim elektronskim servisima u administrativnim okvirima.

4.6 Primena u zdravstvenoj zaštiti i osiguranju

Sistem zdravstvene zaštite i osiguranja jedne zemlje je po pravilu glomazan i skup, pa svaka automatizacija značajno unapređuje poslovanje i snižava troškove. SMART kartice mogu biti primenjene u oblasti zdravstvenog osiguranja i oblasti zdravstvene zaštite (*kao zdravstveni kartoni i profesionalne kartice zaposlenih*).

Primena elektronskih zdravstvenih kartona utiče na sniženje troškova smanjenjem broja nepotrebnih ispitivanja, testiranja pacijenata i izdavanja lekova. Unapređuje se poslovanje većom raspoloživošću i pokretljivošću podataka uz visok nivo njihove zaštite i strogo utvrđenu hijerarhiju pristupa ličnim i poverljivim podacima.

Zdravstvena kartica sadrži osnovne podatke o vlasniku, oznaku krvne grupe, eventualne alergije i hronične bolesti, a doktor upisuje svaku posetu, dijagnozu i primenjen lekarski tretman za pacijenta, čime se izbegava dupliranje napora, a nekada i lekarskih tretmana pri promeni lekara, zdravstvene ustanove ili mesta boravka, a naročito pri hitnim intervencijama. S druge strane, vlasnik zdravstvene kartice je siguran da samo kvalifikovana i ovlašćena lica mogu pristupiti njegovim podacima. Doktor ima viši nivo ovlašćenja za pristup podacima od laboranta ili apotekara, na primer. Da bi pristupio podacima smeštenim u čipu zdravstvene kartice, doktor mora koristiti svoju profesionalnu karticu sa PIN brojem koja verifikuje njegova prava za pristup podacima.

4.7 MEĐUNARODNI ZAHTEVI, PREPORUKE I STANDARDI

Neporeciva veza između fizičkog i elektronskog identiteta je neophodan uslov za izgradnju kvalitetnih i pouzdanih servisa u sistemu elektronske uprave (*servisu za efikasno obavljanje upravnih poslova elektronskim putem preko Interneta*).

U dokumentima Evropske unije koji se odnose na izgradnju sistema Elektronske Evrope (*e- Europe*) ključni zahtev je da se obezbedi razmena elektronskih dokumenata koji su pravno validni i imaju obavezujuću snagu za obe strane u komunikaciji (*sa jedne strane je to državni aparat koji ima ulogu davaoca usluga, a sa druge strane građani i privreda koji imaju ulogu korisnika tih usluga*), kao ključni uslov za primenu kritičnih servisa elektronske uprave preko Interneta.

Prema dokumentima EU, elektronski dokumenti imaju istu pravnu snagu kao i standardni papirni dokumenti ukoliko su primenjeni propisani sistemi za njihovu zaštitu. EU Direktiva ultimativno zahteva od svih članica da ovakvim elektronskim dokumentima ne mogu osporiti pravnu valjanost.

Posebno treba napomenuti skup servisa elektronske uprave koji su identifikovani kao tačke u kojima je neophodno ugraditi sistem zaštite. Neki od servisa zahtevaju samo identifikaciju učesnika a neki pored uspostave autentičnosti lica zahtevaju i njegov elektronski potpis. Zbog toga je u okviru elektronske uprave potrebno realizovati IAS²¹ servise klijenta koji koriste infrastrukturu PKI digitalnih sertifikata.

Po preporukama Evropske komisije primarni elektronski identifikacioni dokument trebalo bi koristiti kao SSCD²² za generisanje kvalifikovanih elektronskih potpisa.

EU direktiva definiše uslove koji su neophodni da bi se generisali kvalifikovani elektronski potpisi. PKI tehnologija i smart kartice koje se primenjuju za eID²³ u potpunosti ispunjavaju postavljene uslove.

Prilikom uvođenja ITS eID veoma je važno da se poštuje evropska pravna regulativa (*jer je ona najnaprednija po pitanju zaštite privatnosti i pitanju obrada ličnih i poverljivih podataka*) definisana sledećim direktivama i odlukama Evropskog parlamenta i Saveta Ministara:

- Direktiva 95/46/EC od 24.X 95. je glavni referentni propis za koncept eID i tiče se zaštite privatnosti lica po pitanju obrade ličnih i poverljivih podataka i njihovog slobodnog kretanja.
- Direktiva 97/66/EC od 15.XII 97 tiče se obrade podataka i zaštite privatnosti u telekomunikacionom sektoru.
- Direktiva 99/93/EC od 13.XII 99. godine reguliše standarde za digitalni potpis.
- Direktiva 00/31/EC od 08. VI 00. reguliše pravne okvire za elektronsku trgovinu.
- Direktiva 01/45/EC reguliše standarde za elektronsku administraciju, odnosno elektronske transakcije sa državnim institucijama i organima.
- Odluka 01/497/EC reguliše standarde za zaštitu ličnih podataka u transakcijama van EU.

²¹ IAS - Identification, Authentication & Signature

²² SSCD - Secure Signature Creation Device

²³ eID - elektronski identifikacioni dokument

Evropsku elektronsku inicijativu je pokrenula Evropska komisija, odnosno eEurope Smart Card Charter, decembra 1999.god i cilj je proširenje oblasti primene smart kartica među zemljama EU, uz poboljšan postupak utvrđivanja i dokazivanja identiteta i unapređenje zaštite podataka u elektronskim transakcijama, zasnovan na biometriji.

Višenamenska primena eID znači korišćenje dokumenta ne samo za dokazivanje identiteta, već i za druge namene. Memorija čipa ID pruža mogućnost smeštanja različitih aplikacija. To može biti kombinacija eID sa drugim dokumentom ili korišćenje za elektronske usluge. Moguće primene su u zavisnosti od nacionalne zakonske regulative (*izdavaoca eID*), razvijenosti i rasprostranjenosti elektronskih servisa, kao i samog vlasnika dokumenta, jer data višenamenska primena se zasniva na dobrovoljnoj osnovi.

Međunarodna primenljivost znači da eID, izdat u jednoj zemlji, po jednom tehničko - tehnološkom postupku, bude prihvaćen u međunarodnim razmerama, a ujedno da pruža dovoljan stepen sigurnosti za sve učesnike u elektronskim transakcijama (*izdavalac, vlasnik eID, pružalac elektronskog servisa*). Takođe, primer je i korišćenje eID kao putne isprave u zemljama EU.

Evropu možemo smatrati predstavnikom SMART card tehnologije i evropska elektronska inicijativa je veoma jaka. Nju je pokrenula Evropska komisija, odnosno eEurope Smart Card Charter, decembra 1999. godine i cilj je proširenje oblasti primene SMART kartica među zemljama EU, uz poboljšan postupak utvrđivanja i dokazivanja identiteta i unapređenje zaštite podataka u elektronskim transakcijama, zasnovan na biometriji. Ciljna grupa su vlade evropskih zemalja i njihove institucije za izdavanje ID i donošenje propisa, kao i prodavci softvera i pružaoci elektronskih usluga.

Radi kroz 12 radnih grupa (*za javni identitet, identifikaciju i autentikaciju, profile zaštite i sertifikate, čitače kartica, elektronska plaćanja, beskontaktna SMART kartice, višenamenske SMART kartice, zahteve korisnika, javni transport, servis elektronske vlade, zdravstvenu primenu i elektronski potpis*).

Cilj radne grupe za javni identitet je:

- uvođenje servisa elektronske vlade među članicama EU,
- povećanje poverenja u elektronske transakcije povećanjem bezbednosti transfera podataka, i
- promocija evropske trgovine.

Porvoo eID Group je osnovana u aprilu 2002. godine, i čine je tehnički i pravni eksperti iz oblasti državne uprave 19 zemalja. Sastaje se svakih 6 meseci radi razmene informacija u pogledu razvoja koncepta ili primene koncepta ID baziranih na SMART karticama sa PKI u svojim zemljama. Cilj ove grupe je utvrđivanje minimuma zahteva za korišćenje elektronskog identiteta osobe van granica jedne zemlje i razvoj sigurnih elektronskih transakcija (*usluga e-vlade, e-bankarstva, e-trgovine...*).

EUCLID inicijativa direktno podržava nastojanja eEurope Smart Card Charter-a i sarađuje direktno sa radnom grupom za javni identitet. Cilj je razvoj e-vlade i e-trgovine baziranim na sigurnim transakcijama.

Prilikom uvođenja ITS eID veoma je važno da se poštuje evropska pravna regulativa, jer je ona najnaprednija po pitanju zaštite privatnosti i pitanju obrada ličnih i poverljivih podataka.

4.8 DOMAĆI PROPISI

Učesnici u organizaciji izdavanja eID su: država ili policija kao izdavaiaac identifikacionog dokumenta, registraciono telo (RA)²⁴ koje utvrđuje identitet budućeg vlasnika identifikacionog dokumenta propisanim sredstvima pre izdavanja sertifikata i eID kartice i sertifikaciono telo (CA)²⁵ koje izdaje i povlači digitalne sertifikate.

Država kao izdavalac ima glavnu odgovornost u izdavanju eID i njena uloga se sastoji u:

- koordinaciji rada CA i RA,
- pravnom regulisanju obaveza i odgovornosti između CA i RA u postupku izdavanja ID,
- obavezi da prilagodi nacionaino zakonodavstvo novom eID (*zakone o ličnim dokumentima i zakon o digitainom potpisu i druge zakone*) i
- razmatranju mogućnosti uključivanja drugih aplikacija.

Registraciono telo utvrđuje identitet budućeg vlasnika identifikacionog dokumenta propisanim sredstvima (*digitalna kamera, skener otiska prsta...*), pre izdavanja sertifikata i kartice, direktno utvrđuje identitet prema fizičkom izgledu i, ukoliko je moguće, evidentira sve osobene znake i prosleđuje korisnički zahtev za izdavanje ID Sertifikacionom telu, te u tom smislu predstavlja posrednika između podnosioca zahteva i sertifikacionog tela.

Sertifikaciono telo izdaje sertifikate prema propisanom postupku iz Direktive 1999/93/EC za elektronski potpis, povlači sertifikate, odgovorno je za izdati sertifikat i dužno je da nadoknadi eventualne štete nanete pravnom ili fizičkom licu koje mogu biti izazvane korišćenjem tako izdatog sertifikata.

eID pruža mehanizam pouzdane provere identiteta i utvrđivanja autentičnosti vlasnika kartice pri korišćenju elektronskih servisa (*e-vlade, e-poslovanja, e-bankarstva, e-trgovine*) javnoj administraciji i pružaocima elektronskih usluga. To se postiže tehnikom digitalnih sertifikata koja se zasniva na infrastrukturi javnih kjučeva i asimetričnoj kriptografiji.

Digitalni sertifikat je dokaz elektronskog identiteta jednako kao što je dokument sa fotografijom dokaz identiteta u svakodnevnom životu. CA ga izdaje na osnovu prethodno proverenog identiteta po pouzdanom i sigurnom postupku.

Sertifikat za digitaino potpisivanje garantuje neporecivost podataka. Potpis se verifikuje korišćenjem javnog kjuča ovog sertifikata i bilo kakvo naknadno menjanje podataka više nije moguće, što je i cilj digitainog potpisivanja - neopozivost elektronske transakcije.

Takođe mogu biti smešteni i sertifikati sa odgovarajućim privatnim ključevima za druge elektronske usluge radi pouzdane veze korisnik usluge - pružalac usluge.

²⁴ RA - Registration Authority

²⁵ CA-Certificate Authority

Da bi ovo funkcionisalo pružaoci elektronskih usluga treba da imaju poverenja u izdavaoca sertifikata (*Sertifikaciono telo*), što se postiže odgovarajućom organizacijom izdavanja elektronskih ID i sertifikata, kao što je prethodno izloženo.

Osim toga, zainteresovane strane moraju da dobiju sve potrebne podatke iz sertifikata, počev od podatka o važenju sertifikata do informacije o digitalnom potpisu.

Iz tog razloga, izdavanje sertifikata mora poštovati direktivu EU koji reguliše izdavanje digitalnih sertifikata i njihovu upotrebu (*Direktivu 99/93/EC*), kao i propisani minimum podataka na sertifikatu.

Svaki sertifikat eID-a ima sledeće podatke:

- ime Sertifikacionog tela,
- ime vlasnika ID,
- jedinstveni identifikacioni broj vlasnika,
- period važnosti izdatog sertifikata,
- serijski broj sertifikata,
- svrhu sertifikata i
- druge tehničke informacije neophodne za korišćenje izdatog sertifikata.

Propisani minimum podataka poštovaće svaki izdavalac sertifikata i podržavati svaka aplikacija kao deo protokola o prenosu podataka.

Sertifikati koje izdaje Sertifikaciono telo, kao i root sertifikat koji identifikuje samog izdavaoca sertifikata, mogu biti memorisani na elektronskoj ID kartici.

Provera (verifikacija) sertifikata:

- U cilju verifikacije izdatog sertifikata, aplikacija koju koristi vlasnik eID kartice „čita“ sertifikat sa eID kartice i potom ga „predaje“ pružaocu elektronske usluge kao deo protokola o prenosu podataka.
- Softver pružaoca usluge zatim „čita“ i tumači sve podatke iz sertifikata (*definisane propisanim minimumom podataka na sertifikatu*).

Validacija sertifikata:

Prvi korak u validaciji, odnosno utvrđivanju važenja i ispravnosti sertifikata je korišćenje javnog ključa Sertifikacionog tela.

Da bi se to izvelo na pouzdan način, Sertifikaciono telo mora da pruži bezbedan kanal za dostavljanje njenih sertifikata do pružaoca usluge.

Takođe, važna je i provera validnosti izdavaoca sertifikata, što se postiže proverom sertifikata koji identifikuje Sertifikaciono telo (*root certificate*) preko web sajta Sertifikacionog tela.

Pružalac usluge mora imati odgovarajući zaštitni softver koji će čuvati integritet memorisanih sertifikata.

Dobijanje informacija o statusu sertifikata:

Sledeći korak u validaciji sertifikata je provera da sertifikatu nije istakla važnost ili da nije povučen.

Zato je obaveza Sertifikacionog tela da pruži pouzdan i lako dostupan servis za utvrđivanje ili proveru statusa sertifikata.

Sertifikaciono telo može izdavati kompletnu CRL²⁶ listu, tj. listu povučenih sertifikata, u određenim pravilnim intervalima, ili da pruži jedan OCSP²⁷ servis, on-line servis za proveru statusa sertifikata (*koji radi u realnom vremenu*).

U Republiki Srbiji je Zakon o elektronskom potpisu usvojen 20. decembra 2004. godine i njime je uvedena pravna regulativa za uvođenje u primenu kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog sertifikata.

²⁶ CRL - Certificate Revocation List

²⁷ OCSP - Online Certificate Status Protocol

4.9 STANDARDIZACIJA

ISO/IEC²⁸ se bave međunarodnom standardizacijom uopšte. Grupa JTC-1²⁹ u okviru ISO/IEC se bavi utvrđivanjem standarda u oblasti informacione tehnologije, a u okviru ove grupe potkomitet SC17 je zadužen za donošenje standarda za izdavanje identifikacionih dokumenata baziranih na smart karticama i utvrđivanje elektronskog identiteta lica. Standardi koje ISO/IEC propisuje u ovoj oblasti su:

- ISO/IEC 7816 kao glavni dokument koji određuje standarde u pogledu fizičkih osobina kontaktnih smart kartica (*takođe i ISO/IEC 7810, ISO/IEC 7813*)
- ISO/IEC 14443 i ISO/IEC 15693 određuju standarde za bezkontaktne SMART kartice
- ICAO³⁰ je veoma uticajna organizacija koja trenutno obuhvata 188 zemalja i zadužena je za donošenje standarda za putne isprave (*pasoši, vize i boravišne dozvole*). ICAO standard 9303 reguliše standarde za mašinski čitljive putne isprave, i integrisan je sa ISO/IEC 7501. ICAO se trenutno bavi standardizacijom novih viza i elektronskih putnih isprava, koji uključuju najsavremenije zaštitne mehanizme (*bezkontaktni poluprovodnički čip sa biometrijskim podacima i antenu*).

Postoje različite biometrijske standardizacione inicijative koje se tiču kako biometrijskih podataka na samoj kartici, tako i razmene takvih podataka.

- BioAPI³¹ standard pruža jedan visokokvalitetni model biometrijske autentikacije i to nezavisno od primenjene tehnologije. On pokriva kako funkcije za upisivanje biometrijskih podataka na karticu i u bazu, verifikaciju i identifikaciju, tako i standarde za interfejs za bazu biometrijskih podataka.
- CBEFF³² je biometrijski standard koji se tiče razmene i međunarodne primenljivosti biometrijskih podataka.

Po pitanju zaštite i bezbednosti IS odgovor na pitanje: „Koliko je dati sistem siguran i koja je cena toga?“ odgovor daju zaštitni standardi:

- ITSEC³³ standard po pitanju sistema zaštite je donet 1991. godine u Evropi
- USA (TCSEC) i Kanada (CTCPEC) su razvile različite standarde.
- Nedavno je donet Common Criteria standard (ISO/IEC 15408), koji širom sveta predstavlja punovažan sigurnosni standard i koji objedinjuje sve navedene sigurnosne inicijative
- ITSEC i Common Criteria imaju različite skale vrednosti
- Svaki proizvod odnosno komponenta u ITS eID (*ugrađeni čip na smart kartici, operativni sistem na čipu, PKI sistem, operativni sistem za bazu podataka, fire-walis...*) može biti vrednovan po navedenim skalama.
- ITSEC i Common Criteria (CC) pružaju efikasan postupak za procenu sigurnosti proizvoda, ali se očekuje skori preiatak samo na primenu Common Criteria standarda u vrednovanju nivoa sigurnosti pojedinih komponenti u ITS.

²⁸ISO/IEC - Međunarodna organizacija za standardizaciju i Međunarodna elektrotehnička komisija

²⁹JTC-1 - Joint Committee 1

³⁰ICAO - International Civil Aviation Organization

³¹BioAPI - Biometric Application Program Interface

³²CBEFF - Common Biometric Exchange File Format

³³ITSEC - Information Technology Security Evaluation Criteria

4.10 ZAKLJUČAK

Zbog porasta kriminalnih dela u vezi zloupotrebe identiteta, a u poslednje vreme i zbog straha od terorističkih akcija među donosiocima odluka u mnogim vladama i poslovnim organizacijama u svetu, sve je manje podeljenih mišljenja u shvatanju važnosti i ozbiljnosti pitanja sigurnog i pouzdanog utvrđivanja identiteta. Razvojem novih, naprednih tehnologija, pre svega tehnologije SMART kartica i biometrijske tehnologije i njihovim uključivanjem u utvrđivanje i proveru identiteta lica, svet će neizbežno postati mnogo komplikovaniji osobama koje se bave zloupotrebom identiteta. Sve to znači razvoj sigurnih i pouzdanih elektronskih transakcija odnosno razvoj usluga e-vlade, e-trgovine, e-poslovanja, e-bankarstva... putem Interneta.

Građani će moći da efikasno opšte sa vladinim servisima, da kupuju proizvode elektronskim putem bez straha od mogućih zloupotreba, putnici će putovati brže i lakše prelaziti granice, preduzeća će biti u prilici da omoguće svojim radnicima obavljanje poslova sa udaljenih mesta, potpuno sigurna da samo oni mogu pristupiti određenim podacima.

Brzo će doći dan kada će pitanje pouzdanog utvrđivanja identiteta konačno zauzeti drugorazredni značaj, ali ne kao nevažno, već stoga što će taj postupak postati javan i siguran, tako da će krivična dela zloupotrebe identiteta postati prošlost.

GLAVA V

5 IDENTIFIKACIONI DOKUMENTI

5.1 UVOD

Vlade širom sveta susreću se sa sve ozbiljnijim problemom kontrole populacije i njene migracije. Identifikacija populacije je temelj nacionalne sigurnosti. Glavni ciljevi savremenog identifikacionog sistema su:

- efikasna granična kontrola,
- pouzdano legitimisanje na javnim mestima
- sigurnost u trgovinskom i administrativnom poslovanju.

Kao odgovor na ovaj problem, informatičke kompanije širom sveta poslednjih godina razvijaju centralizovano / decentralizovane sisteme za masovnu produkciju visoko zaštićenih identifikacionih dokumenata građana.

Ovakvi sistemi su bazirani na četiri osnovna koncepta:

- digitalizacija svih podataka koji se pojavljuju na identifikacionim dokumentima (*fotografija, otisak, tekst i dr.*)
- centralizovana produkcija koja garantuje najvišu zaštitu
- visok produkciono nivo (*izrada do 5000 dokumenata u jednom satu po produkcionoj mašini*)
- realizacija standardizovanih tehnologija izrade dokumenata po pitanju materijala, zaštite, kvaliteta, estetike i drugih elemenata

Sve navedeno je potpuno integrisano u nove produkcione sisteme koji danas uključuju:

- radne stanice za prikupljanje svih podataka putem aplikacionih formi ili direktno
- visoko produkcione mašine za izradu dokumenata na bazi unapređenih tehnologija laserskog štampanja
- visoko produkcione mašine za laminaciju i sečenje dokumenata koje u potpunosti eliminišu potrebu za direktnim učešćem operatora
- sisteme za kvalitativnu kontrolu procesa koje mogu automatski prepoznavati - čitati bar kod odn. OCRB karaktere odn. neke druge standardne mehanizme.

Odmah na početku da se razumemo. Ja nisam pobornik teorija zavere čipovanja ljudi i smatram da je digitalizacija dokumenata dobar put. Međutim, to ne znači da ne treba ignorisati potencijalne probleme. Naša javnost je već neko vreme prepuna svakojakih apokaliptičnih komentara vezano za digitalizaciju ličnih karata i pasoša koji su uglavnom posledica nerazumevanja tehnologije.

5.2 IDENTIFIKACIONI DOKUMENTI KOD NAS

Po novoj tehnologiji izdavanja, lična karta postaje osnovni dokument za potvrdu identiteta, odnosno predstavlja primarni identifikacioni dokument. Svi ostali dokumenti (*putna isprava, vozačka dozvola, saobraćajna dozvola...*) spadaju u sekundarne identifikacione dokumente i služe za potvrdu podataka koji su u njima navedeni, te njihovo korišćenje uključuje interaktivno ili direktno korišćenje primarnog ID. Putna isprava se može smatrati primarnim ID kada se koristi u inostranstvu, dok se za korišćenje u zemlji ona smatra sekundarnim ID. Osnovni uslov za izdavanje bilo kog sekundarnog identifikacionog dokumenta je postojanje primarnog. Time je procedura za izdavanje sekundarnog dokumenta pojednostavljena i ubrzana, jer se zasniva na već prikupljenim alfanumeričkim i biometrijskim podacima lica.

Projekti nove putne isprave, vozačke dozvole, saobraćajne dozvole, dozvole za nošenje oružja i drugih sekundarnih dokumenata zasnovanih na tehnologiji „pametnih“ kartica su u fazi pripreme i realizacije.

5.3 KARAKTERISTIKE DOKUMENATA

Elektronska lična isprava je multiaplikativna PKI kontaktna SMART kartica sa različitim operativnim sistemima, softverskim i hardverskim mehanizmima za zaštitu (*algoritmima sa kriptografskim ključevima, hardverskim generatorom ključeva na čipu...*) i funkcijama bezbednog čuvanja podataka i ovlašćenog pristupa.

Ona sadrži:

- vidljive (*na kartici*) i nevidljive (*u čipu*) tekstualne i biometrijske podatke vlasnika,
- asimetrične privatne ključeve (*za digitalni potpis i digitalnu envelopu*) i dva digitalna sertifikata koji odgovaraju tim ključevima,
- mašinski čitljivu zonu,

Sve u cilju neporecive identifikacije vlasnika dokumenta i tačnosti podataka na dokumentu.

Elektronska putna isprava sadrži:

- vidljive tekstualne i biometrijske podatke vlasnika,
- mašinski čitljivu zonu,
- 2D bar kod sa nevidljivim tekstualnim i biometrijskim podacima,

- podatke na beskontaktnom čipu prema LDS³⁴ specifikaciji.

Dokumenta su po standardima ICAO 9303, ISO/IEC standardima, preporukama i direktivama EU, a u skladu sa domaćim i međunarodnim pravnim aktima.

5.3.1

Istina ili ...

Mnogo se pričalo i pisalo o elektronskim ličnim kartama, ali je veliki deo tih informacija bio u potpunosti ili delimično netačan, što je izazivalo veliku konfuziju. Objasniću neke osnovne stvari i mogućnosti novih dokumenata...



Slika 32 Nova LK u čitaču

Lična dokumenta, znamo, služe za identifikaciju njihovih nosilaca, pa je važno da budu jedinstveni, što se postiže na dva načina:

- posebnim procesom proizvodnje blanko medijuma koji treba da bude (*gotovo*) nemoguć za kopiranje i
- unošenje ličnih podataka nosioca u taj blanko medijum.

Lična karta je dokument „izveden“ iz registra svih građana, čiji je jedinstveni identifikator JMBG³⁵. I pored stalnih povika na razne mogućnosti zloupotreba i napada na privatnost, ne treba posebno objašnjavati potrebu svake države da ima kompletnu evidenciju svojih građana - bez toga bi nastao haos u svim domenima života i poslovanja. I države poput SAD i Velike Britanije, koje se često navode kao primeri zemalja koje nemaju lične karte (*mada su sada u procesu uvođenja*), imaju njen ekvivalent (*u SAD to je vozačka dozvola*), kao i ekvivalent JMBG-a, a to je čuveni social security broj, jedinstveni broj socijalnog osiguranja. Dakle, samo su nazivi malo drugačiji.

³⁴ LDS - Logical Data Structure

³⁵ JMBG - jedinstveni matični broj građana

Povremeno nailazim na pitanja koja se svode na „šta će nam uopšte lične karte?“. Da li želimo da se neko (*obično zlonamerno*) predstavlja kao mi, da, recimo, može da pristupi našem bankovnom računu, otvori bankovni račun ili firmu na naše ime, odvede naše dete iz vrtića ili škole, da se leči na naše ime, da budemo uhapšeni umesto nekog drugog? Da ne pominjemo impersonalizaciju na Internetu, o čemu slušamo već par decenija. Mogućnosti zloupotrebe su velike i za običnog čoveka često šokantne, ali su deo realnosti. Kreatori „preposlednjih“ ličnih karata sigurno nisu mogli da sagledaju dokle će dogurati tehnika, niti čime će sve raspolagati fizičko lice današnjice, što kao posledicu ima relativno jednostavnu i jeftinu mogućnost kopiranja lične karte.

Nova lična dokumenta su definitivno potrebna, i moraju biti takva da se ne mogu praviti „na svakom ćošku“, kopirati ili izdavati sa netačnim informacijama, čak ni od strane zaposlenih u ovlašćenoj ustanovi koja ih izdaje. Dokumenta, u skladu sa današnjim načinom života, moraju obezbediti pouzdanu identifikaciju i kada „sa druge strane“ ne sedi službenik, već smo za računarom.

5.3.2

Proizvodnja lične karte

Aspekte novih ličnih karata ćemo najlakše obuhvatiti ako objasnimo proces njihove proizvodnje. Zbog velikog napretka tehnike, bilo kakve papirne varijante kao osnovni materijal za proizvodnju ličnih dokumenata više ne dolaze u obzir - sva nova dokumenta u svetu prave se u obliku i dimenzijama platnih kartica. Standardizacija dimenzija i oblika je važna, jer se sve više koriste sa mašinama za razne namene (*npr. čitači kartica, bankomati i univerzalni kompjuterski „kiosci“*). Izuzetak je za sada pasoš, koji iz praktičnih razloga (*vize i nedostatak savremene infrastrukture na graničnim prelazima*) mora da ima papirne strane.

Materijal koji se nametnuo kao najbolji izbor za osnovu elektronskih dokumenata današnjice je polikarbonat, koji ima neke osobine keramike, a proizvodi ga svega nekoliko kompanija u svetu. Savremena lična karta ima telo od desetak slojeva polikarbonata, od kojih su neki odštampani osnovnim obrascem, pa je postupak proizvodnje vrlo složen. Da sve bude komplikovanije, postoji razlika zavisno od toga da li je izabran dokument sa čipom ili bez njega - onaj sa čipom nema polje na kome se nalazi adresa prebivališta, što je za rezultat imalo zvaničnu obavezu svih ustanova koje rade sa ličnim kartama da nabave čitače kartica.



Slika 33 Pametna kartica

Bilo je mnogo spekulacija u vezi s mogućnošću (*ne*)željenog očitavanja ovakvih dokumenata. S obzirom na to da je u pitanju kontakti čip, nema načina da se očitavanje izvrši sa daljine - za čitanje sadržaja kartica se mora „ubosti“ u čitač. Čip koji se koristi na ličnim dokumentima spada u najzaštićenije uređaje koji su ikada napravljeni i zadovoljava najrigoroznije svetske kriterijume (*CC EAL 5+ standard, ima više elemenata zaštite pristupa čipu i kriptografske kontrole*).

Čak i u svim novim (*elektronskim*) pasošima, glavna strana (*na kojoj su lični podaci nosioca*) je napravljena od polikarbonata. Kad smo već kod elektronskih pasoša, napomenimo da su oni drastično različiti u odnosu na elektronske lične karte, ne samo izgledom već i elektronski - čitaju s beskontaktnim uređajima. Lične karte poseduju skup elemenata zaštite čipa koji se između ostalog zasniva na simetričnim i asimetričnim kriptografskim protokolima i ograničenju pristupa podacima. Ovi elementi zaštite pažljivo su projektovani da bi se obezbedila zahtevana sigurnost uz praktičnost upotrebe. Ovakvi sigurnosni mehanizmi odabrani su, između ostalog, iz savremenih specifikacija i potreba koje propisuju svetske organizacije koje se bave pitanjima ličnih karata, elektronskih pasoša i platnih (*bankarskih*) kartica sa čipom.

Proces proizvodnje i izdavanja elektronskih dokumenata prati evidencija svakog parametra, koja ne dozvoljavaj a malverzacije, ni ljudi koji su u direktnom kontaktu sa proizvodnim procesom, niti onih van njega. S obzirom na osetljivost operacije, svaka „blanko kartica“ dobij a serijski broj pre nego što izađe iz mašine, a one sa čipom dobijaju i serijski broj čipa, u potpuno automatizovanom procesu. Na taj način se u svakom trenutku zna gde se koja kartica i čip nalaze, i zajedno sa njenim statusom evidentiraju se u posebnim bazama podataka. Ove informacije se upotpunjuju sa svakom promenom statusa kartice, uključujući i njeno uništenje (*u slučaju da ne prođe kontrolu kvaliteta, ili one kojoj je istekao rok važenja*), čime se eliminiše mogućnost manipulisanja škartom.

Postoji puno pasivnih komponenti zaštite ličnih dokumenata, a svaka država sama bira one za koje smatra da su joj potrebni i dizajnira odgovarajuće grafičke elemente. Naše lične karte ih imaju desetak, među kojima su kinegram (*vrsta holograma*), giljoš (*mnoštvo tankih krivih linija u različitim bojama koje zajedno daju kompleksnu sliku u pozadini, odštampanu u veoma visokoj rezoluciji*), MLI (*višestruka laserska slika*), ghost image (*umanjena originalna slika nosioca u crno-belom tehnici*)...

Na poleđini lične karte je i trolinijska mašinski čitljiva zona - MRZ³⁶ sa ličnim podacima, koja je predviđena za skeniranje i pouzdano prepoznavanje karaktera OCR³⁷. Na taj način, čak i ako ne postoji mogućnost čitanja podataka iz čipa, moguće je osnovne podatke pročitati mašinski i tako eliminisati prekucavanje, što se uglavnom sprovodi na graničnim prelazima.

³⁶ MRZ - Machine Readable Zone

³⁷ OCR - Optical Character Recognition

5.4 Lična karta

Za razliku od sveta, u Srbiji će se biometrijski pakovati samo podaci koji su se i do sada prikupljali pri vađenju ličnih dokumenata, a nove lične karte sa čipom za sada su opcione...



Slika 34 *Prednja strana nove LK*



Slika 35 *Druga strana LK bez čipa*

Nova lična karta je plastična kartica slična platnim karticama. Nakon izdavanja, na njoj su odštampani lični podaci, fotografija i potpis građanina. Na poledini je i takozvana „mašinski čitljiva zona“, odnosno tri reda teksta koji se može „pročitati“ optičkim prepoznavanjem teksta.



Slika 36 *Blanko obrazac - prednja strana*



Slika 37 Blanko obrazac sa čipom - druga strana

Na kartici se nalazi čip u kom su lični podaci. Očitavanje čipa je kontaktno, provlačenjem kartice kroz odgovarajući uređaj - čitač „smart“ kartica. Čip je marke Infineon, kapaciteta 32 KB. Na čip lične karte u MUP-u se zapisuju alfanumerički podaci (*ime, prezime, JMBG, adresa, eventualna promenjena adresa prebivališta itd.*). Karticu nazivamo biometrijskom zbog toga što sadrži jedinstvene fiziološke podatke o osobi: fotografiju (*JPEG napravljen od donesene slike ili od fotografije lica snimljene u MUP-u*), otiske prstiju (*zapisane u standardnom formatu za tu namenu, koji sadrži izgled otiska, ali i, da tako kažemo, „analiziran“ i kompresovan izgled otiska*). Takođe, na čip se snima i slika svojeručnog potpisa građanina. Verovatno najvažnije, i u budućnosti najkorisnije za građane, na novoj ličnoj karti nalazi se i tzv. elektronski potpis vlasnika kartice.

Inače, lična karta može biti i u varijanti kartice bez čipa, ako građanin tako želi, o čemu se izjašnjava prilikom izdavanja nove lične karte.

U lične karte je ugrađen čip koji se može pročitati isključivo kontaktim čitačem. To znači da karta mora da se stavi u čitač da bi je on pročitao. To uslovljava fizički kontakt sa ličnom kartom. Podaci na njoj su trećem licu dostupni samo ako ono ima pristup ličnoj karti, a to nije ništa više opasno nego i kada staru ličnu kartu damo nekome da je pročita ili priložimo fotokopiju.

Čip ne sadrži ništa opasnije od podataka koji i inače stoje odštampani na običnoj ličnoj karti. Postojanje čipa samo olakšava celu proceduru - umesto da neko kome trebaju naši podaci prepisuje sa nje, jednostavno je provuče kroz čitač i svi podaci su prepisani.

Pogodnost je što se provera dokumenata može vršiti mnogo brže, čak i potpuno automatizovano, a to nije u korist samo policije, kako se to obično tumači, već jednostavno znači da svaka procedura koja sadrži i potrebu čitanja podataka iz ličnih dokumenata može biti značajno ubrzana. Za nas, to znači manje gubljenja vremena na šalterima i čekanju u redovima.

Kada se uzme u obzir da je planirano da se lična karta koristi i kao dokument za elektronski potpis, to znači da ćemo moći da mnoge poslove obavimo preko Interneta, jer ćemo moći da potvrdimo svoj identitet bez fizičkog prisustva na nekom šalteru.

U stvari jedini problem sa ličnim kartama sa čipom je u tome što se neko „dosetio“ da, pošto su podaci upisani u čip, oni ne moraju biti odštampani na karti, tako da ako imate ličnu kartu sa čipom, a onaj kome podaci trebaju nema čitač, imaćete problem - jer je tada lična karta beskorisna.

Umesto da se i na čipovanim kartama odštampanju potrebni podaci, neko se opet „dosetio“ da naredi da svi kojima je potrebno da prikupljaju podatke iz ličnih karata moraju da nabave čitače. Nije teško zaključiti da je tako obezbeđeno da onaj ko proizvodi (ili uvozi) čitače tako ima zagarantovanu sjajnu zaradu. Zar nije jednostavnije odštampati na ličnu kartu te podatke koji su neophodni?

5.4.1

Biometrija i dokumenta



Slika 38 Nova biometrijska LK



Slika 39 Stara LK

Da se o strahu od moguće zloupotrebe više priča u medijima nego što panika postoji među ljudima, govori podatak da je tokom prve godine izdavanja novih ličnih karata, tek manje od 10% građana rešilo da izbegne čip.

5.4.2

Skeniranje bioloških osobina

Čip, odnosno „kontaktni mikrokontroler“, u stvari je konvertor koji analogni signal prebacuje u digitalni, tako da ga PC razume. Naravno, on sadrži i podatke, a njih sa nove lične karte niko neće moći da „očita sa daljine“, već će biti potrebno to učiniti mašinskim putem.

Biometrija je metoda prikupljanja podataka radi autentifikacije i ima mnogo širu primenu nego što je to predviđeno novim dokumentima građana Srbije, koji će ostati bez većine karakteristika nosioca dokumenta kao što su skeniranje rukopisa, glasa, ruke, lica, zenice, DNK zapisa ili čak načina na koji pritiskamo tastaturu. Primera radi, u Japanu je zakonom regulisano da se, radi bezbednosti i identifikacije, u bankama koristi skeniranje vena na rukama, što očitavaju kamere sa infracrvenim senzorom. Jedino što će novi čip u ličnim kartama sadržati od biometrijskih podataka je ono što već ostavljamo prilikom podnošenja zahteva za prvu ličnu kartu - fotografiju, otisak prsta i potpis. To da će sloboda biti oduzeta usled automatizacije pri prikupljanju i čitanju biometrijskih podataka moglo bi da važi samo za begunce pred zakonom, jer bi trebalo da nove lične karte pruže značajan doprinos borbi protiv kriminala i falsifikovanja isprava.

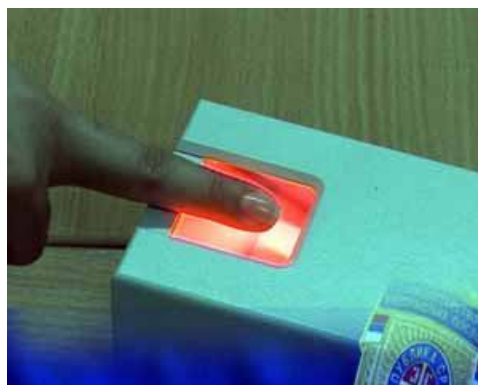
5.4.3

Personalizacija

Kada osoba pokrene proceduru izdavanja nove lične karte, u MUP-u se preuzimanju negovi ili njeni lični podaci, građanin se fotografiše (*u odgovarajućoj kabini*) i uzimaju mu se otisci oba kažiprsta, uz poređenje sa podacima koji su već u sistemu (*ako postoje*). Ovi podaci se smeštaju u odgovarajuće baze podataka i obrađuju, da bi se pripremili za smeštanje u buduća dokumenta u procesu personalizacije, koja se vrši u dve faze - vizuelnoj i elektronskoj.



Slika 40 Tabla za potpis



Slika 41 Skener za otisak prsta

U vizuelnoj, svi lični podaci, **ghost slika, otisak prsta i potpis** se upisuju laserom, i to na jednom od unutrašnjih slojeva kartice. Štampa se i slika lica u boji, posle čega sledi laminacija, koja sprečava grebanje spoljnih slojeva u toku upotrebe. Ukoliko lična karta poseduje čip, sledi takozvana elektronska personalizacija.

Sadržaj čipa je vrlo često bio predmet fantaziranja novinara. Zapravo, u njemu se nalaze isti podaci o nosiocu koje vidimo na samoj ličnoj karti, plus adresa stanovanja, (*koja, ako se promeni, ne zahteva zamenu elektronskog dokumenta*). Tu su i fotografija (*u nižoj rezoluciji od odštampane*) i minucije oba kažiprsta. Minucije su skupovi značajnih tačaka otisaka prsta, a proces njihovog dobijanja je jednosmeran - iz minucije ne možete dobiti originalni otisak.

Svi ovi podaci se digitalno potpisuju, što isključuje mogućnost neopažene promene podataka u čipu, jer je za validan digitalni potpis neophodna oprema koju ima samo organizacija koja vrši personalizaciju.

Poslednje što se upisuje u čip su digitalni sertifikati i kriptografski ključevi, namenjeni digitalnom potpisivanju i šifrovanju podataka. Posebno je značajan ključ namenjen digitalnom potpisivanju, jer se on generiše u samom čipu lične karte i nikada ga ne napušta - operacija digitalnog potpisivanja obavlja se u samom čipu. On predstavlja još jedan važan faktor novih ličnih karata, a to je da su privatnost i identitet nosioca zagarantovani, jer ovaj ključ ne postoji čak ni u evidenciji izdavaoca ličnih karata.

Naravno, mora postojati i način zaštite nosioca u slučaju gubitka lične karte, što se rešava korišćenjem tajne šifre, tj. primenom uobičajene metode da nešto imate, a nešto pamтите. Na taj način, čak i ako neko (*neovlašćeno*) dođe u posed naše lične karte, neće moći da nas impersonira elektronskim putem, kao što se radi sa platnim karticama.

Poslednji korak u proizvodnji i izdavanju elektronske lične karte je njeno pakovanje u zapečaćeni koverat, zajedno sa listom papira sa osnovnim podacima, kao i upisanom sistemski generisanom slučajnom šifrom (*niz slova i brojeva*) koja se mora uneti pri digitalnom potpisivanju ili drugim osetljivim operacijama. Ne treba isticati da je ovaj korak, u stvari, kraj potpuno automatizovanog procesa proizvodnje. Zapakovana dokumenta šalju se na mesta gde je predviđeno njihovo izdavanje nosiocima.

5.4.4 Personalizacija dokumenata

Ova faza predstavlja izradu primarnog identifikacionog dokumenta i upisivanje ličnih i drugih podataka na dokument. Uključuje:

- Elektronsku personalizaciju, odnosno upisivanje alfanumeričkih i biometrijskih podataka iz baze i generisanih digitalnih sertifikata na čip kartice,
- Vizuelnu personalizaciju, odnosno izradu kartice i štampanje vidljivih podataka na samoj kartici, i
- Ugrađivanje hardverskih i softverskih zaštitnih mehanizama

Pakovanje dokumenta i pripadajućeg PIN broja se vrši u posebne dve koverte.

5.4.5 Zašto čip?

Videli smo šta se u čipu nalazi, ali ne i kako sve on unapređuje ličnu kartu, osim što otežava kopiranje. Čip donosi dve glavne prednosti nosiocu - jedna je mogućnost pouzdane identifikacije putem Interneta, a samim tim i autorizacije različitih operacija. Druga je

pretvaranje lične karte u univerzalni identifikacioni token, što omogućava da se upotrebljava za npr. kontrolu radnog vremena, pristup računaru i druge stvari za koje je do sada bilo normalno da se upotrebljava posebna kartica (*ili neki drugi token*).

Autorizacija putem Interneta znači obavljanje mnogih operacija od kuće, sa posla ili sa bilo koje tačke na svetu. Prva primena, na koju smo već navikli, jeste elektronsko bankarstvo - (*šta će nam posebna kartica koja se posebno plaća, ističe posle nekog vremena i predstavlja još jednu stvar koju treba da nosimo i o kojoj treba da mislimo?*) Odmah zatim dolaze i postupci kao što su vađenje i produžavanja raznih potvrda i dokumenata, kao i predaje završnih računa, za koje sada mora da se ide u opštinu, MUP ili neko treće mesto, da se čeka u beskrajinim redovima, gundđa na šalterske radnike koji bi uvek „mogli to i brže“, izlazi sa posla i, generalno, gubi vreme.

Čak i kada dođemo na neki šalter, uskoro više neće biti prepisivanja naših podataka iz lične karte u računar, već će oni u trenutku biti prebačeni automatski, što pored ubrzanja eliminiše i mogućnost greške. Iako ima mnogo skeptika, mnogi projekti ovog tipa su već u pripremi, a prvi koji će biti pušteni u rad su servisi elektronske vlade. Zamislimo koliko će se na taj način, kada servisi zažive, uštedeti vremena i živaca (*dovoljno je da uporedimo sa elektronskim bankarstvom*). Da ne pominjemo postojeće inicijative na svetskom nivou koje omogućavaju upotrebu ličnih karata kao univerzalnih tokena za pristup svim nalogima koje pojedinac ima na Internetu - zbogom username i password.

Postoje i mnoge prednosti ovako sofisticiranih sistema u domenu suzbijanja kriminala. Recimo, kada policija ligitimiše neku osobu, odmah će proveriti da li je to lice iz nekog razloga traženo, na osnovu čega policajac odmah može da reaguje na pravi način. Nažalost, i izdavanje saobraćajnih kazni će biti mnogo brže...

5.4.6

Korist od novih dokumenata

Šta bi to konkretno značilo za građane, a koju bi korist od toga imala naša država. Izvesno je da lakša identifikacija, pa samim tim i komunikacija, štedi vreme, što znači i novac. Kada je reč o novim pasošima, mislim da je to pitanje, nezavisno od nas, apsolvirano u međunarodnim okvirima: još pre nekoliko godina, prvo SAD a potom i EU donele su propise kojima su etablirane biometrijske putne isprave. Biometrijski pasoš postao je uslov za nesmetano kretanje na ogromnom prostoru.

Baza podataka „Memorija Srbije“ nalazi se ulici Kneza Miloša i zameniće kilometre papirnih dokumenata, a pristup će biti moguć samo autorizovanim licima, i to tek nakon prolaska kroz bezbednosnu proceduru. Jedan od razloga za brigu predstavlja raskorak između biometrijskih dokumenata i regulative koja bi obezbedila zaštitu privatnosti podataka.

Na faktičkom planu nemamo skoro ništa. Nije slučajno da se u dokumentima posmatrača EU konstatuje da zaštita podataka o ličnosti u Srbiji postoji samo kao teorijski fenomen. Možda je nelogično da budemo jedna od prvih evropskih zemalja koja uvodi pametne lične karte, a poslednja koja nije donela savremen i funkcionalan zakon o zaštiti podataka o ličnosti.

5.4.7**Distribucija dokumenata**

Uručivanje dokumenta je preko mreže registracionih mesta na kojima se i prikupljaju zahtevi za izradu dokumenta (*službeni kurir dostavlja dokument registracionom telu koje ga uručuje*).

Ako se uručenje dokumenta vrši preko registracionog mesta, postupak je sledeći:

- Ovlašćeni službenik pronalazi zahtev u informacionom sistemu i personalizovan dokument.
- Verifikuje dokument, vezu dokument - lice i lice.
- Vršiti dopersonalizaciju dokumenta za potrebe korišćenja elektronskog ID dokumenta u budućem sistemu elektronske uprave. Ovlašćeni službenik pokreće aplikaciju za generisanje para ključeva (*javni/privatni*) i dobijeni javni ključ šalje Sertifikacionom telu preko interaktivne veze, kao zahtev za dobijanje digitalnog sertifikata.
- Ovlašćeni službenik evidentira datum uručjenja.

5.5 Postupak izdavanja identifikacionog dokumenta

Postupak izdavanja identifikacionog dokumenta je opisan na primeru primarnog identifikacionog dokumenta. Provera identiteta i ovlašćenja registracionog službenika se vrši putem službene eID. Postupak izdavanja primarnog identifikacionog dokumenta se odvija se na sledeći način:

Nakon prijema zahteva za izdavanje propisanih dokumenata ovlašćeni službenik vrši: proveru dokumenata (*da li su sva potrebna dokumenta priložena i da li su originali, potpisana, overena pečatom, sa ispravnim rokom važenja*), proveru veze dokument - lice (*vizuelno poređenje fotografije lica iz dokumenta i izgleda čoveka*) i proveru lica (*vizuelno poređenje fotografije lica, ako je priložena, i izgleda podnosioca zahteva*) i vrši evidentiranje zahteva za izdavanje dokumenta.



Slika 42 Proizvodna traka LK



Slika 43 Pakovanje LK

Akvizicija podataka obuhvata unos tekstualnih podataka iz zahteva za izdavanje dokumenta podnosioca, skeniranje otisaka prstiju pomoću skenera za uzimanje otisaka, fotografisanje lica pomoću digitalne kamere, akviziciju potpisa pomoću table za digitalizaciju potpisa, akviziciju priloženih dokumenata skeniranjem. Nakon toga ovlašćeni službenik evidentira zahtev i izdaje potvrdu o tome.

U ovoj fazi je moguća izmena podataka i upis novih podataka na čipu kartice (*npr. izmena adrese*) ili smeštanje aplikacija za korišćenje servisa elektronske vlade - odnosno dopersonalizacija dokumenta.

Odlučivanje o zahtevu se odvija u sledećim koracima:

Verifikacija je postupak poređenja dva uzorka (1:1), trenutno formiranog na prijemnom mestu i prethodno sačuvanog iz kartona poslednje izdate LK. Uzorak može biti jedinstveni matični broj građana, broj dokumenta ili otisak prsta. Verifikacija obuhvata:

- Verifikaciju dokumenta (*proveru autentičnosti dokumenta*),
- Verifikaciju veze dokument - lice (*da li biometrijski podaci iz dokumenta odgovaraju podnosiocu zahteva*),
- Verifikaciju lica (*poredi se skeniran otisak prsta sa onim iz kartona poslednje izdate LK ili informacionog sistema*).

Identifikacija je postupak pronalaženja uzorka u skupu od više elemenata ($1:N$), radi pronalaženja eventualnih zloupotreba i falsifikata, odnosno otkrivanja da jedno lice poseduje više dokumenata ili da više lica koriste dokument sa istim brojem. Uzorak može biti jedinstveni matični broj građana, broj dokumenta ili otisak prsta. Identifikacija obuhvata:

- Identifikaciju dokumenta (*proveru dokumenta u evidencijama izdatih dokumenata i međunarodnim evidencijama krađenih i falsifikovanih dokumenata*). Ako se dokument ne nalazi u evidenciji izdatih dokumenata ili se nalazi u evidenciji krađenih blanko dokumenata, to ukazuje na zloupotrebu;
- Identifikaciju veze dokument - lice (*proveru dokumenta u evidencijama izdatih dokumenata i međunarodnim evidencijama krađenih i falsifikovanih dokumenata*). Npr. evidencija falsifikovanih dokumenata može da sadrži više dokumenata sa istim serijskim/registarskim brojem, ali svaki sa drugim identitetom, ili propisno izdat dokument, ukraden i sa izmenjenim podacima o identitetu;
- Identifikaciju lica (*provera uzetog otiska sa podacima iz baze biometrijskih podataka radi pronalaženja potencijalno dvostrukog identiteta*).

Obrada zahteva za izdavanje dokumenta obuhvata:

- Upis ili izmenu tekstualnih podataka o licu u evidencijama vezanim za identitet podnosioca, ako postoji razlika između novoprikupljenih podataka i prethodno sačuvanih u evidencijama. Izmena ličnih podataka vidljivih na dokumentu (*JMBG, imena, prezimena*) ima za posledicu zamenu identifikacionog dokumenta;
- Dopunu podataka podacima iz sekundarnih identifikacionih dokumenata (*oružni list, npr.*).

Ovlašćeni registracioni službenik formira skup podataka za personalizaciju (*prema strukturi zakonski važećeg identifikacionog dokumenta*) i digitalno ih potpisuje.

Kriptovanje odnosno šifriranje podataka primenom tehnologije digitalne envelope. Šifrirani podaci se šalju do centralne baze podataka.

Priprema zahteva za izdavanje dokumenta. Nakon smeštanja podataka u centralnu bazu generiše se nalog za personalizaciju.

Priprema podataka za proces personalizacije obuhvata: Generisanje kriptografskih parametara za zaštitu, odnosno:

- Podaci se dodatno šifriraju specijalnim simetričnim ključem.
- Generiše se par asimetričnih ključeva (*privatni/javni*) za sertifikat za enkripciju podataka (*digitalna envelope*), a privatni ključ se smešta u pripadajuću bazu podataka. Funkcija ovih ključeva je za slučaj gubitka, krađe ili kvara dokumenta, radi dešifrovanja podataka pripremljenih u odgovarajućoj instituciji državne uprave, a koji su šifrovani postupkom digitalne envelope na bazi digitalnog sertifikata date osobe.
- Šalje se zahtev za generisanje digitalnog sertifikata (*koji sadrži javni ključ*) Sertifikacionom telu interaktivnom zaštićenom vezom.
- Generiše se PIN broj (*korisničko ime i lozinka*) za datu osobu.
- Formiranje izlaznih podataka za datu osobu, njihovo šifriranje, digitalno potpisivanje i slanje personalizacionom centru u zahtevanom formatu.

5.6 Izdavanje elektronskog identifikacionog dokumenta

Subjekti u izdavanju su:

- Država kao izdavalac ima glavnu odgovornost u izdavanju eID, ona:
 - Koordinira rad Sertifikacionog (CA) i Registracionog tela (RA),
 - Pravno reguliše obaveze i odgovornosti između CA i RA u postupku izdavanja ID,
 - Ima obavezu da prilagodi nacionalno zakonodavstvo novom eID (*zakon o ličnim dokumentima, zakon o digitalnom potpisu i druge zakone*),
 - Razmatra mogućnost uključivanja drugih aplikacija.
- Registraciono telo - RA:
 - Utvrđuje identitet budućeg vlasnika identifikacionog dokumenta propisanim sredstvima (*digitalna kamera, skener otiska prsta...*), pre izdavanja sertifikata i kartice,
 - Identitet utvrđuje direktno, prema fizičkom izgledu i, ukoliko je moguće, evidentira sve osobene znake budućeg vlasnika eID,
 - Prosleđuje korisnički zahtev za izdavanje ID Sertifikacionom telu, te u tom smislu predstavlja posrednika između podnosioca zahteva i Sertifikacionog tela.
- Sertifikaciono telo - CA:
 - Izdaje sertifikate prema propisanom postupku iz Direktive 1999/93/EC za elektronski potpis,
 - Povlači sertifikate,
 - Odgovorno je za izdati sertifikat i dužno je da nadoknadi eventualne štete nanete pravnom ili fizičkom licu koje mogu biti izazvane korišćenjem tako izdatog sertifikata.

5.7 KORIŠĆENJE eID

Odgovornost za čuvanje eID -

Vlasnik je obavezan da čuva eID i PIN broj prema uslovima određenim ugovorom između vlasnika kartice i izdavaoca lične isprave radi sprečavanja eventualnih zloupotreba. PIN broj ne sme da se čuva na istom mestu kao i eID.

Druge aplikacije na eID -

Upisivanje dodatnih aplikacija u slobodnoj memoriji čipa mora biti zaštićeno PIN-om i/ili biometrikom. Preporučuje se da svaka aplikacija ima svoj poseban PIN. Smeštanje aplikacija i poništavanje njihove upotrebe mora biti pravno regulisano između vlasnika kartice i pružaoca elektronske usluge.

Produženje eID

Rok važnosti izdatog eID i pripadajućih sertifikata propisuje država izdavalac (5-10 god). Preporučuje se da rok važnosti dokumenta i sertifikata bude jednak.

Produženje važnosti kartice i sertifikata treba da bude pravno regulisano i da se vrši po odgovarajućoj i sigurnoj proceduri, kao i njihovo izdavanje. Svaka upisana aplikacija na eID je u nadležnosti vlasnika kartice koji je zadužen za njen prenos na produženu ID karticu.

Sertifikaciono telo može izdavati kompletnu CRL³⁸ listu, tj. listu povučenih sertifikata, u određenim pravilnim intervalima, ili da pruži jedan OCSP³⁹ servis, on-line servis za proveru statusa sertifikata.

Verifikacija i validacija sertifikata -

Sertifikati koje izdaje Sertifikaciono telo, kao i root sertifikat koji identifikuje samog izdavaoca sertifikata, mogu biti memorisani na elektronskoj ID kartici.

Provera (verifikacija) sertifikata -

Aplikacija koju koristi vlasnik eID kartice, „čita“ sertifikat sa eID kartice i potom ga „predaje“ pružaocu elektronske usluge kao deo protokola o prenosu podataka. Softver pružaoca usluge zatim „čita“ i tumači sve podatke iz sertifikata (*definisane propisanim minimumom podataka na sertifikatu*).

Utvrđivanje važenja i ispravnosti sertifikata (validacija) sertifikata -

Prvi korak u validaciji sertifikata je korišćenje javnog ključa Sertifikacionog tela. Sertifikaciono telo mora da pruži bezbedan kanal za dostavljanje njenih sertifikata do pružaoca usluge. Važna je i provera validnosti izdavaoca sertifikata, što se postiže proverom sertifikata koji identifikuje Sertifikaciono telo (*root certificate*) preko web sajta Sertifikacionog tela. Pružalac usluge mora imati odgovarajući zaštitni softver koji će čuvati integritet memorisanih sertifikata.

5.7.1

Iskustva drugih zemalja

Prva država koja je primenila elektronske lične karte na čitavu populaciju je Estonija, koja je proces zamene počela još 2004. godine. Sve lične karte imaju čip i intenzivno se krenulo u uvođenje elektronskih servisa, koji su uštedeli vreme i novac kako ljudima tako i državi, kroz smanjenje troškova na potrošni materijal, koji su izuzetno veliki. Ne zaboravimo da u elektronskim transakcijama praktično nema papira, tonera za štampače... Primer Estonije su sledile Finska, Belgija i druge države.

Slovenija, koja je nešto kasnije počela sa uvođenjem elektronskih ličnih dokumenata, danas prednjači na evropskom i svetskom nivou, zahvaljujući pravilnom pristupu razvoju infrastrukture i prevođenju svih podataka u elektronski oblik, što omogućava vrlo jednostavno uvođenje svih potrebnih servisa. Nisu u pitanju samo elementarne usluge. Ko hoće da dobijete

³⁸ CRL - Certificate Revocation List

³⁹ OCSP - Online Certificate Status Protocol

dozvolu za izgradnju kuće, - nema razloga da ustaje sa stolice, - sve će obaviti putem računara i servisa na Internetu! Sada predstavljaju primer svim zemljama kako treba raditi, da ne pominjemo velike privredne efekte koji proizilaze iz konsaltinga i projekata koje njihove firme rade u drugim zemljama. A kod nas se 2009. ljudi pitaju „**zašto mi da budemo prvi?**“.

5.7.2 Biometrijska dokumenta u regionu

Kada su u pitanju pasoši, trenutno se mogu koristiti tri biometrijska podatka:

- izgled lica,
- otisak prsta i
- „otisak“ dužice.

Formate biometrijskih fajlova i komunikacione protokole definiše ICAO koja je agencija Ujedinjenih nacija. Naravno, u pasošima se ne moraju naći sva tri biometrijska podatka, a u praksi se i ne nalaze.

Evropska zajednica planira da u biometrijskim pasošima ima upisan izgled lica i otisak prsta. Izgled lica bio je obavezan da se nađe u pasošima do avgusta 2006. godine, a otisak prsta će morati da bude ubačen u pasoše do juna 2009. godine. Tehničke specifikacije e-pasoša određuje Evropska komisija, a obavezujuće su za sve zemlje članice, izuzev Danske, Irske i Velike Britanije, kao i zemalja Evropske ekonomske oblasti Islanda, Norveške i Švajcarske. Neke zemlje su već uvele i drugi nivo biometrijske zaštite, tako da nemački pasoši noviji od novembra 2007. godine imaju u sebi i po otisak prsta sa svake ruke.

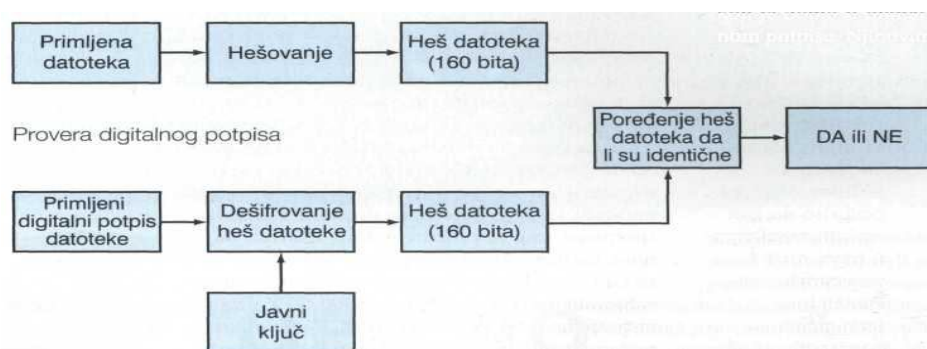
Makedonski biometrijski pasoši izdaju se od aprila 2007. godine i koštaju 25 evra. Crnogorski e-pasoši počeli su da se izdaju od maja 2008. godine, a koštaju 40 evra. Hrvatska i Bosna i Hercegovina još nemaju biometrijske pasoše. U BiH planiraju da uvedu e-pasoš polovinom sledeće godine, a u Hrvatskoj je uvođenje novih dokumenata isto planirano za 2009. godinu, ali postoji ideja da se objedine lična karta i pasoš u jedan dokument.

Što se ličnih karti tiče, situacija je nešto drugačija nego kada su u pitanju pasoši. U mnogim zemljama vode se debate o tome da li lične karte predstavljaju način države da prati kretanje i postupke svojih građana. Kada se u celu priča doda i pridev „biometrijska“, stvari postaju još gore. Ukoliko postoje elektronske lične karte, na njih se ugrađuju smart kartice koje omogućavaju čitanje podataka samo preko kontakta namenskim čitačem. Situacija u Evropi toliko se razlikuje od zemlje do zemlje da ću navesti samo dva ekstrema. U Belgiji svaki stanovnik stariji od 12 godina mora da ima neki vid identifikacije sa sobom, a od 2000. godine sve lične karte imaju čip u sebi. Nasuprot tome, u Danskoj, građani po zakonu ne moraju ni da imaju ličnu kartu. Danska državna kartica zdravstvenog osiguranja je nešto najbližije tome, ali na njoj ne postoji slika, čipove da i ne pominjem. Lične karte sa čipom koriste se u Španiji od 2006. godine, a planirane su za uvođenje u Italiji u narednim godinama.

Sa čipom ili bez njega? Apsolutno, sa! Nema razloga da se zazuje od nečega što samo može da nam pomogne.

5.8 DIGITALNI POTPIS

Jedan od najznačajnijih servisa koje omogućava kriptografija javnih ključeva predstavlja kreiranje digitalnog potpisa. Digitalni potpis elektronskog dokumenta je analogan pisanom potpisu na papirnom dokumentu, jer jedan entitet može potpisati neke podatke a neograničen broj entiteta taj potpis može pročitati i proveriti njegovu ispravnost. Digitalni potpis je neuporedivo sigurniji od rukopisnog, jer je praktično nemoguće da bilo koji drugi entitet kreira potpis identičan npr. onom koji napravi Alis. Drugim rečima, falsifikovanje je neizvodljivo.



Slika 44 Digitalno potpisivanje

Digitalni potpis se oslanja na koncept para ključeva, privatnog i tajnog. Privatni ključ mora postojati, jer je Alisin digitalni potpis jedinstveno vezan samo za nju. Sa druge strane, njen javni ključ mora biti dostupan široj grupi entiteta (*najbolje svima*) da bi mogao na odgovarajući način da se proveri i identifikuje kao Alisin, što se ne može postići sa simetričnim ključem. Digitalno potpisivanje dokumenta (*tj. elektronske datoteke*) se obavlja u dva koraka.

Pošto je veličina samog dokumenta nepredvidljiva (*to može biti e-mail poruka od tri reči kao i datoteka od 50 MB*), a RSA algoritam kojim se vrši digitalno potpisivanje privatnim ključem radi na informaciji fiksne veličine, potreban je neki postupak kojim se od polazne datoteke dobija jedinstveni niz znakova iste dužine. Taj postupak, nazvan hashing, procesiranjem originalne datoteke bilo koje veličine daje jedinstveni rezultat (*hash*) čija je dužina obično 160 bita (*SHA-1 algoritam*). Algoritam za hešovanje je takav da će svaka promena u originalnoj datoteci izazvati promenu i u samom hešu, a realno se ne mogu naći dve različite datoteke koje će dati identičan heš. Drugi korak predstavlja šifrovanje dobijenog heša korišćenjem privatnog ključa, a ta šifrovana informacija predstavlja digitalni potpis dokumenta.

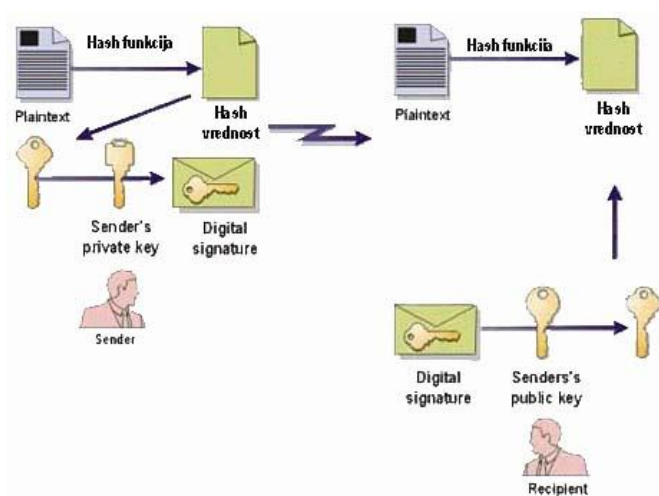
Primalac će, zahvaljujući digitalnom sertifikatu pošiljaoca i njegovom javnom ključu (*koji je uvek sadržan u sertifikatu*), moći da dešifruje digitalni potpis datoteke i da tako dođe do heša. Sa druge strane, primalac će i sam napraviti heš datoteke, i uporediti ga sa onim koji je dobio u digitalnom potpisu. Njihovim poređenjem primalac će moći da proveri da li je poslata datoteka menjana ili ne, jer ova dva heša moraju biti identični. Posebnom proverom digitalnog sertifikata može se utvrditi identitet pošiljaoca i validnost samog sertifikata.

Napomenućemo da ova operacija ne šifrjuje podatke koji se prenose, već se to mora uraditi posebno. U procesu digitalnog potpisivanja učestvuju tri datoteke - ona sa informacijama koje se potpisuju, digitalni sertifikat potpisnika i sam digitalni potpis. Na koji način će one biti čuvane i prenošene posle postupka digitalnog potpisivanja, zavisi od potreba - sve tri mogu biti odvojene, integrisane u jednom fajlu ili kombinovane na neki drugi način.

Digitalni potpis obezbeđuje primaocu vrlo važnu informaciju o integritetu podataka, tj. da li su primljeni i poslani podaci identični. Rezultat je tipa „da“ ili „ne“, dakle ne može se saznati šta je u podacima menjano. Zahvaljujući osobinama heš funkcije, koja daje vrlo različite izlaze i za najmanje promene u ulaznim datotekama, primalac može mirne duše smatrati da su primljeni podaci identični poslatim ako je izlaz procedure verifikacije pozitivan.

Da bi se preneli kriptovani podaci korišćenjem digitalnog potpisa, pošiljalac mora da obavi sledeće operacije:

- Dobije hash vrednost podataka pomoću hash funkcije
- Enkriptuje hash vrednost sa privatnim ključem da bi kreirao digitalni potpis
- Pošalje originalnu poruku i digitalni potpis primaocu
- Da bi dobio podatke u izvornom obliku primalac mora da izvrši sledeće operacije:
- Dobije novu hash vrednost na osnovu dobijene poruke
- Dekriptuje digitalni potpis javnim ključem pošiljaoca, čime dobije originalnu hash vrednost
- Uporedi ove dve hash vrednosti da proveri integritet podataka i identitet pošiljaoca



Slika 45 Identifikacija digitalnim potpisom

5.9 DIGITALNI SERTIFIKAT

Algoritam i ključevi brinu o enkripciji podataka i procesu dekripcije, ali ne zadovoljavaju zahteve za zaštićenom verifikacijom. Bilo ko može generisati javni i privatni ključ. Digitalni sertifikati razrešavaju ovo tako što potvrđuju da je javni ključ koji koristi pošiljaoc, aktuelni javni ključ primaoca. Sertifikaciono telo izdaje sertifikat, koji sadrži identifikacione informacije o vlasniku ključa. Osnovna funkcija sertifikacionog tela je pouzdano uspostavljanje zaštićenog digitalnog identiteta svih učesnika za komunikaciju u nebezbednoj računarskoj mreži. Sertifikaciono telo, takođe, vodi računa o roku važnosti izdatih sertifikata, upravlja povlačenjem sertifikata i objavljivanjem lista povučenih sertifikata.

Tehnologija koju opisujem je izuzetno obimna. To ne iznenađuje ako se prisetimo da je teorijski razvoj njenih osnova počeo još sedamdesetih godina prošlog veka i da intenzivno traje i danas. Njena namena je maksimalno obezbeđivanje identifikacije osoba ili sistema i privatnosti podataka. Mnoge procedure su u čitavom svetu još u razradi, a mogu se i razlikovati u različitim državama.

```

Primer sertifikata

Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town,
           O=Thawte Consulting cc,
           OU=Certification Services Division,
           CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
      Not Before: Jul  9 16:04:02 1998 GMT
      Not After : Jul  9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
            OU=FreeSoft, CN=www.freesoft.org/
            Email=baccala@freesoft.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
          33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
          ...
        Exponent: 65537 (0x10001)
      Signature Algorithm: md5WithRSAEncryption
      93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
      92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
      ...
  
```

Slika 46 Primer sertifikata

Digitalni sertifikat je struktura podataka koja za cilj ima pouzdano povezivanje javnog ključa sa podacima o njegovom nosiocu, obezbeđujući na taj način proveru identiteta pri, na primer, digitalnom potpisivanju. Sertifikat može biti samopotpisani ili kvalifikovani - oni su u tehničkom pogledu jednaki, ali samopotpisani može da vam izda bilo ko, a to možete uraditi i sasvim sami. Uglavnom se koriste interno, ili se pravna snaga dobija potpisivanjem posebnog obavezujućeg ugovora sa korisnikom (*kao u e-banking sistemima*).

Daleko značajniji je kvalifikovani digitalni sertifikat, koji po Zakonu o digitalnom potpisu i pripadajućim podzakonskim aktima može da izda samo sertifikaciono telo koje ispunjava određene zakonske uslove i ima dozvolu za rad. Kvalifikovani digitalni sertifikat sa odgovarajućim parom ključeva se može upotrebiti za kreiranje „kvalifikovanog digitalnog potpisa“ elektronskog dokumenta, koji je po pravnoj snazi ekvivalentan papirnom dokumentu potpisanom na klasičan način - olovkom i pečatom.

Čak i prema pomenutom zakonu, postoji nekoliko izuzetaka od ovog pravila - recimo, prenos prava svojine na nepokretnosti, uređenje imovinskih odnosa između bračnih drugova, ugovori o poklonu, ugovori o doživotnom izdržavanju, sporazumi u vezi sa nasleđem za sada će se potpisivati na klasični način.

5.9.1 Interna struktura

Jedno od najčešćih pitanja u vezi digitalnih sertifikata je „Šta je u njima zapisano?“. Opšteprihvaćeni standard unutrašnje strukture i podataka je X.509, koji je od 1988. godine do danas imao tri verzije. Aktuelna varijanta obuhvata verziju, jedinstveni serijski broj (*jedan od najvažnijih podataka*), ID algoritma za hešovanje, vreme važenja od - do, ID algoritma javnog ključa, sam javni ključ, ID algoritma digitalnog potpisa, digitalni potpis. Opciona su polja: identifikator izdavača, identifikator nosioca i ekstenzije.

Glavno unapređenje u verziji 2 je uvođenje jedinstvenih identifikatora izdavača i nosioca, a u verziji 3 uvođenje tzv. „ekstenzija“. Ekstenzije su važne, jer u suštini omogućavaju da u sam digitalni sertifikat unesemo bilo kakve potrebne podatke. Recimo, tu može stajati informacija o dozvoli za obavljanje nekih poslova ili o pravu potpisa neke vrste ugovora koje ima zaposleni. Sistem koji implementirate ih može prepoznati i reagovati na odgovarajući način. Međutim, ako se prava upisana u ekstenziju izmene, recimo zbog promene radnog mesta, sertifikat mora biti opozvan i nosiocu treba izdati novi.

Zakon jasno propisuje kakve uslove mora da zadovolji uređaj koji se koristi za pravljenje kvalifikovanog digitalnog potpisa. Da ne ulazimo u detalje, mora imati mogućnost generisanja tajnog ključa u sebi (*što zahteva poseban hardver*) i taj ključ nikad ne sme napustiti sam uređaj. Dakle, postupak digitalnog potpisivanja, tj. enkripcije heša se mora obaviti u samom uređaju. Takođe mora da ispunjava stroge uslove zaštite podataka, koji garantuju neuspeh svakog neovlašćenog pokušaja da se iz njega „izvuku“ smešteni podaci i to na bilo koji način (*uključujući i hardverske zahvate*).

5.9.2 Put do sertifikata

Proces izdavanja digitalnog sertifikata počinje u tzv. registracionom autoritetu RA. RA je „istureno odeljenje“ nekog sertifikacionog tela i obično ih ima više jer pokrivaju neku teritoriju, recimo državu. Tu se predaje zahtev za izdavanje koji sadrži lične podatke podnosioca. U RA se zatim vrši provera predatih podataka i, ako ona pokaže da je sve u redu, prelazi se na pripremu zahteva za izdavanje.

Nosilac na licu mesta dobija karticu koja je odštampana ali u sebi ne sadrži ni digitalni sertifikat niti ključeve. Kod kuće, uz priloženi softver, korisnik generiše par javni/tajni ključ na samoj kartici i pokreće proceduru kreiranja zahteva za izdavanje, koja će zahtev upotpuniti potrebnim podacima i napraviti skoro kompletan digitalni sertifikat. Ovako pripremljen dokument se prosleđuje sertifikacionom telu čiji je zadatak samo da ga digitalno potpiše koristeći svoj tajni ključ. Time je formiran kompletan digitalni sertifikat, koji se vraća nosiocu i koji ga, posredstvom posebnog softvera, smešta na svoju karticu. Tajni ključ nikada ne napušta karticu, što je jedan od najbitnijih razloga pouzdanosti ovakvog sistema.

5.9.3 Sertifikaciona tela

Sertifikaciono telo CA je entitet koji digitalno potpisuje primljene zahteve za digitalne sertifikate. Ono je neophodno u procesu izdavanja digitalnih sertifikata, jer predstavlja instituciju kojoj se veruje. Napravimo paralelu sa ličnim kartama - mi u stvari ne verujemo samoj ličnoj karti, kao komadu specijalnog papira, već telu (*država/MUP*) koje ju je izdalo i na osnovu tog poverenja smatramo da su podaci o nosiocu u njoj tačni. Zahvaljujući podatku u samom digitalnom sertifikatu o telu koje ga je izdalo, kreira se „lanac sertifikata“ koji (*ako krenete u proveru*) vodi do „glavnog“ tela kome se veruje.

Kako obezbediti poverenje u neko CA telo? Tako što se realizuje njihova „piramida“, na čijem je vrhu vrhovno državno sertifikaciono telo (*Root CA - kao da je u korenu stabla*). Ono je dobro čuvano, kako fizički tako i elektronski, i ima skup strogih pravila po kojima radi. Za razliku od ostalih, Root CA telo samo sebi potpisuje digitalni sertifikat. U našoj zemlji ono je pod upravom Ministarstva za nauku.

Međutim, od ovog tela se ne može kupiti digitalni sertifikat. Root CA ih izdaje samo tzv. Među - CA telima (*Intermediate CA, kratko ICA*), koja komercijalno izdaju sertifikate. Dakle, korisnici mogu kupiti kvalifikovani digitalni sertifikat samo od ICA tela, kojih će u Srbiji biti nekoliko. Root CA nije univerzalno telo, već se koriste različita za elektronske pasoše, lične karte...

Za normalan rad javnog CA tela neophodan je i skup aplikacija koje omogućavaju upravljanje životnim vekom samog sertifikata. Pored navedenih, moraju da obezbede i različite evidencije i publikovanje informacija, zatim funkcije opoziva i pauziranja sertifikata, kao i obnavljanja - sertifikati obično važe samo jednu godinu (*iz sigurnosnih i ekonomskih razloga*).

Kada već nešto digitalno potpišemo, potrebno je da se ispravnost originalne datoteke i njenog digitalnog potpisa može proveriti. Zato CA tela mogu objaviti podatke o izdatim digitalnim sertifikatima, mada to nije obavezno. Obavezno je objavljivanje informacija svih CA tela o svim njihovim izdatim sertifikatima koji su pauzirani ili opozvani, što se radi kroz liste opozvanih sertifikata - CRL, tj. Certificate Revocation List. U normalnim okolnostima, pri svakoj upotrebi digitalnog sertifikata vrši se provera njegove ispravnosti - prvo se proverava rok važnosti koji je upisan u sam sertifikat, zatim se provere podaci o CA koje je izdalo digitalni sertifikat potpisnika, a na kraju i da li se sertifikat nalazi na CRL-u. CRL je ekstremno važan sigurnosni mehanizam, koji omogućava da se neki sertifikat maltene trenutno opozove i time spreči njegov korisnik u vršenju nedozvoljenih operacija, bez obzira na to gde se na svetu nalazi.

5.9.4 Globalna scena

Već sad postoji realna potreba da se upotreba digitalnog sertifikata ne ograničava samo na pojedine zemlje. Nažalost, sistem koji bi to omogućio za sada ne postoji, pa kada se radi o kvalifikovanim digitalnim potpisima još uvek nema međudržavnog priznavanja.

Ovaj problem će se gotovo sigurno rešavati po vrstama primene. Na listi prioriteta se nalazi elektronski pasoš, koji je po prirodi stvari namenjen internacionalnoj upotrebi. Standarde za elektronske pasoše je izdala organizacija ISO, ali ih je u najvećoj meri u svojim preporukama definisala organizacija za civilnu avijaciju - ICAO. ICAO sada intenzivno radi na razvoju tzv. Public Key Directory-ja, koji će čuvati potrebne podatke svih država u sistemu.

5.10 eID I KVALIFIKOVANI SERTIFIKATI

eID pruža mehanizam pouzdane provere identiteta i utvrđivanja autentičnosti vlasnika kartice pri korišćenju elektronskih servisa (*e-vlade, e-poslovanja, e-bankarstva, e-trgovine*) javnoj administraciji i pružaocima elektronskih usluga.

To se postiže tehnikom digitalnih sertifikata koja se zasniva na infrastrukturi javnih ključeva i asimetričnoj kriptografiji (*omogućava pouzdanu autentikaciju, tajnost, integritet i raspoloživost podataka*).

Elektronski identifikacioni dokument mora imati najmanje dva sertifikata:

- sertifikat za identifikaciju i šifriranje sa parom ključeva (*javni/privatni*), i
- sertifikat za digitalni potpis sa parom ključeva (*javni/privatni*).

Rešenje sa tri para ključeva je takođe valjano, gde se treći par ključeva koristi isključivo za šifriranje.

Pružaoци elektronskih usluga moraju da dobiju sve potrebne podatke iz sertifikata, počev od podatka o važenju sertifikata do informacije o digitalnom potpisu. Iz tog razloga, izdavanje sertifikata mora poštovati direktivu EU (*Direktivu 99/93/EC*) koji reguliše izdavanje digitalnih sertifikata i njihovu upotrebu, kao i propisani minimum podataka na sertifikatu.

Propisani minimum podataka poštovaće svaki izdavalac sertifikata i podržavati svaka aplikacija kao deo protokola o prenosu podataka.

Svaki sertifikat eID-a ima sledeće podatke:

- ime Sertifikacionog tela,
- ime vlasnika ID,
- jedinstveni identifikacioni broj vlasnika,
- period važnosti izdatog sertifikata,
- serijski broj sertifikata,
- svrhu sertifikata i
- druge tehničke informacije neophodne za korišćenje izdatog sertifikata.

Sertifikati koje izdaje Sertifikaciono telo, kao i root sertifikat koji identifikuje samog izdavaoca sertifikata (CA), mogu biti memorisani na elektronskoj ID kartici.

5.11 Elektronski potpis i lična karta

Elektronski potpis pretstavlja egal našem rukom napisanom potpisu na dokumentu. To znači da elektronski potpis ima istu pravnu težinu kao običan potpis i da on garantuje da je osoba koja je elektronskim putem potpisala dokument zaista osoba za koju se predstavlja.



Slika 47 *Blanko obrazac*

Na primer vlasnik elektronskog potpisa će moći da elektronskim putem potpiše neki dokument i pošalje ga e-mailom na primer u sud, MUP... Taj dokument će imati istu pravnu snagu kao i da je dokument ručno potpisan.

Ovo je jako bitno i za elektronsko poslovanje u Srbiji jer će sada sajtovi koji se bave prodajom roba i usluga imati garanciju da su registrovani kod nadležnog organa i da imaju pravnu odgovornost. To znači da mogu da odgovaraju za eventualne prevare, nepoštovanje ugovora...

Postoji i negativno mišljenje pravoslavnih vernika i crkve o ovoj vrsti dokumenata. Oni kažu da je ovo isuviše blizu opisu iz biblije gde se kaže da će antihrist označiti svakog čoveka brojem i da će čak doći dan da ljudi neće moći da kupuju ni prodaju ako nemaju svoj specijalni broj što i nije tako daleko od istine.

O pojmu elektronskog potpisa pisali smo nekoliko puta i nećemo detaljnije objašnjavati kao funkcionise, jer to nije primarna tema ovog teksta. To što svaki građanin (*koji to želi*) može da ima elektronski potpis, koji mu garantuje dokaz identiteta jer je izdat od strane države, glavna je prednost nove lične karte, jer širom otvara vrata konačnom zamahu elektronske uprave. Kao što mnogi od nas već mesecima ne zalaze u ekspoziture banaka i pošta, tako ćemo uskoro, nadamo se, moći da zaboravimo i na sve ostale šaltere, redove i neljubazne službenike.

5.11.1**Nije komplikovano**

Potpisivanje dokumenata elektronskim potpisom jednostavna je procedura i isto je kao i potpisivanje naloga u elektronskom bankarstvu, koje je u Srbiji rasprostranjeno.

Potpisivanje elektronskog ugovora će funkcionisati na sledeći način: uđemo u MS Word, napišemo tekst ugovora i odaberemo opciju „sajn“, odnosno „potpiši“, dobićemo poruku da ubacimo kartu u čitač i upišemo pin kod i taj dokument je od tog trenutka potpisan. Na potpisanim dokumentima navedeno je ko ih je potpisao i njih ne može menjati ni autor teksta ni primalac.

5.11.2**Potpis mnogo košta**

PTT Srbije par godina građanima izdaje elektronske potpise koji imaju pravnu snagu svojeručnog potpisa. Cena izdavanja potpisa prvi put je 6.500 dinara što uključuje opremu, poput kartice i čitača, dok će se korišćenje elektronskih potpisa naplaćivati 2.000 dinara godišnje.

Elektronski potpis se se može izvaditi u pošti po naknadi od 2.000 din, ali sada se dobija i UZ LIČNU KARTU! To znači da će vlasnici novih biometrijskih ličnih karata imati i elektronski potpis koji je pohranjen u istoj. Elektronski potpis mogu imati pravna i fizička lica.

Zakon o elektronskom potpisu usvojen je 2004. godine, a pravilnik o izdavanju kvalifikovanih elektronskih potpisa usvojen je ove godine.

Za sada samo PTT ima dozvolu za izdavanje kvalifikovanih elektronskih potpisa, a Privredna komora Srbije najavila je da očekuje da će do marta dobiti dozvolu i da će besplatno podeliti potpise svojim članovima da bi podstakla elektronsko poslovanje.

5.12 Novi srpski pasoš - novo lice Srbije

Priča o novim generacijama ličnih dokumenata počela je od pasoša koji se trenutno, slično elektronskim ličnim kartama, nalaze pod „rafalnom paljbom“ javnosti, koja (*opet*) dobrim delom ne razume čitav koncept. Pa da zavirimo u novu putnu ispravu...



Slika 48 Novi pasoš

Svi znamo čemu pasoši služe, a opet smatramo da se problemi krađe identiteta dešavaju „nekom drugom“. Svi smo upoznati sa pričom čoveka, kada je krenuo sa porodicom na more u Grčku, na grčkoj granici saznao da je neko sa njegovim starim pasošem, ukradenim nekoliko godina ranije, izvršio više teških prekršaja i da mu je stoga zabranjen ulaz u zemlje Evropske unije. Ne treba mnogo objašnjavati kolika je to bila neprijatnost, koja je mogla da se završi i mnogo gore. Stoga je jasno da je osnovno pitanje koje se postavlja pred nove, elektronske (*ili kako se često nazivaju - biometrijske*) pasoše - kakav nivo zaštite identiteta pružaju svom nosiocu.

Pošto je „hajka“ na elektronske pasoše uglavnom usmerena na mogućnosti njihove zloupotrebe u smislu kopiranja i promene podataka o nosiocu, pođimo od postojećeg stanja i razmotrimo razlike u odnosu na sadašnje pasoše. Naravno, i „stari“ pasoši imaju zaštitne mehanizme (*specijalan papir, serijski broj zumban na svim stranama, strane pokrivene slikama sastavljenim od kompleksnih spletova linija...*) koje nije lako zaobići, ali se napredak tehnike odrazio i na te mogućnosti. Osnovni problem je što je zamenom fotografije nosioca (*mada je ona zaštićena hologramskom nalepnicom i vodenim pečatom*) moguće preuzeti nečiji identitet i pokušati prelaz preko granice. Stvar otežavaju vize država koje na njima štampaju i fotografiju onoga kome je izdata (*npr. SAD i zemlje potpisnice šengenskog sporazuma*), ali ako je pasoš prazan, maltene nema dalje prepreke. Samo netreba misliti da je srpski pasoš neinteresantan kriminalcima i da smo stoga „mirni“...

5.12.1 Kako je počelo

Do pre samo nekoliko godina slične probleme su imale i ostale zemlje, ali kao da toj problematici nije posvećivana prevelika pažnja. Sve se promenilo posle događaja 11. septembra 2001. godine, zbog čega je SAD objavio rat terorizmu. Jedan od osnovnih uslova

da sprečite teroriste da uđu u vašu zemlju jeste da pojačate kontrolu granica, ali je to pojačanje sa istom infrastrukturom davalo ograničene efekte. Ako bi se koristila nova, naprednija vrsta putnih dokumenata, proces bi bio neuporedivo efikasniji...

Tako je zatraženo uvođenje biometrijskih podataka u pasoše, što umnogome smanjuje mogućnosti falsifikovanja, pa je bilo potrebno napraviti studiju o novim putnim dokumentima, zajedno sa načinom uvođenja. Pri tom je trebalo održati „vertikalnu kompatibilnost“ sa postojećim pasošima, jer je teško očekivati da sve zemlje odjednom zamene sve pasoše. Pošto su u Americi aerodromi ekstremno prometni, organizacija ICAO koja deluje pod organizacijom Ujedinjenih nacija, formirala je radnu grupu koja je propisala nove standarde za elektronske pasoše.

Da čela stvar ne bi ostala mrtvo slovo na papiru, američka administracija je 2002. godine donela zakon po kome sve zemlje čijim građanima nisu potrebne vize za ulazak u SAD moraju da počnu da izdaju elektronske pasoše u roku od dve godine, inače će im vize biti uvedene. Na osnovu odluka samita u Solunu 2003. godine, savet EU je krajem 2004. doneo odluku o uvođenju zajedničkih bezbednosnih standarda i biometrijskih podataka u pasoše i ostala putna dokumenta izdata od strane država-članica. Ozbiljnost namera Amerike je potvrđena i u praksi na primeru npr. Italije, čiji su građani imali period obaveze vađenja viza za ulazak u SAD jer nisu na vreme počeli da koriste nove elektronske pasoše. Do kraja 2006. godine većina evropskih zemalja je počela da izdaje pasoše novog tipa, sa čipom i biometrijskim podacima, a do sada se u taj „klub“ učlanilo oko pedeset zemalja, među kojima je i Srbija.

5.12.2

Novi pasoši

Inače, novi pasoš je „carsko“ crvene boje, a na koricama su ime i grb Republike Srbije, natpis „pasoš“ napisan ćirilicom u zlatnoj boji, kao i oznaka da je pasoš biometrijski, dok je na unutrašnjoj strani korica natpis „Srbija“ naizmenično ćirilicom i latinicom, koji će biti vidljivi samo na ultraljubičastom svetlu.

Pored prve, i druga strana je polikarbonatska, kao na kreditnim karticama, a na prvoj strani je na srpskom, francuskom i engleskom napisano „pasoš“. Druga stranica sadrži lične podatke vlasnika (*fotografija, ime, prezime, mesto i datum rođenja, serijski broj i ostale podatke koje ima i sadašnja isprava*).

Prema elementima zaštite, novi pasoš se najviše razlikuje od starog i ima sedam nivoa zaštite, što ga čini jednim od najmodernijih u Evropi, a novina je i nevidljivi čip s biometrijskim podacima vlasnika.

Novi srpski pasoš, pored drugačijeg izgleda i standardnih mera zaštite od falsifikovanja, sadrži karakteristike po standardu usvojenom u većini evropskih zemalja. Unutar jedne stranice pasoša, koja je nešto deblja, nalaze se Philipsov čip kapaciteta 72 KB i RFID predajnik. Očitavanje pasoša je beskontaktno, tj. može se očitati iz relativne blizine, što je upravo najvažnija odlika RFID tehnologije. Međutim, ovde moramo da napomenemo to da pasoš u našem džepu niko ne može da očita bez našeg znanja, jer je beskontaktno očitavanje moguće tek nakon što pasoš predate na očitavanje „mašinski čitljive zone“, tj. ona famozna tri reda teksta i brojeva koji se prepoznaju optički. Naša policija u čip novih pasoša zasad upisuje alfanumeričke podatke o vlasniku i fotografiju, a uskoro na pasošu će biti pohranjeni i otisci prstiju.



Slika 49 Druga strana pasoša

Iako se mnogo polemike vodi upravo zbog čipa, počnimo od same pasoške knjižice. Unapređenje u odnosu na prethodnu je drastično, gledajući kako po zaštitnim elementima tako i po lepoti. Giljoš linijske strukture koje predstavljaju poleđinu svake strane ne samo da su sada daleko složenije i u različitim bojama, već su i reljefne. Više štampanih elemenata sadrži tekst koji se vidi samo pod određenim uglom, a nekoliko elemenata se vide samo gledajući kroz stranu, kada je ona okrenuta prema svetlu. Pasoš i dalje ima 32 strane, ali se u to ne računa glavna (*holder pagey sa podacima o nosiocu*) a izbačena je i strana za upis maloletne dece koja sada moraju da vade pasoše radi putovanja u inostranstvo, pa ima nešto više mesta za pečate i vize. Sve strane su perforirane serijskim brojem.



Slika 50 Unutrašnje stranice novog srpskog pasoša

Vize će se i dalje izdavati na klasičan način, kao nalepnice, ali će u budućnosti biti sve češće izdavane u elektronskoj formi. Za sada nekog holograma u tom smislu nema, jer nema ni neophodne infrastrukture za njihovo izdavanje i očitavanje, a ni posao oko samih e-pasoša nije ni blizu gotov.

Glavna strana je napravljena od polikarbonata, što je slično ličnim kartama. Lični podaci se upisuju laserom na nekom od unutrašnjih slojeva, a tu su još i višestruka laserska slika (*MLI*), hologram koji je pozicioniran i preko crno-bele fotografije, mikro-tekst (*koji takođe prelazi i preko fotografije nosioca*), giljoš linije i drugo. Strana je zaštićena i od „premeštanja“ u drugi pasoš.



Slika 51 Princip novih biometrijskih pasoša

Pri dnu strane je važna novost, dvolinijska mašinski čitljiva zona, u kojoj su u obliku slova i cifara smešteni najvažniji podaci o nosiocu. Ovakvu zonu smo već mogli da vidimo na vizama zapadnih zemalja, a ima je i na novoj ličnoj karti. Ona omogućava brz prelaz preko granice na kojoj se evidentiraju sve osobe. Iz starog pasoša, umesto da se samo stavi na poseban čitač koji će skenirati MRZ a zatim ga automatski „pročitati“, podaci moraju da se prekucavaju ručno, što je dugotrajan proces. Pored toga, čitači pasoša skeniraju glavnu stranu u tri prolaza, korišćenjem bele, ultravioletne i infracrvena svetlosti, jer se određeni grafički elementi u materijalu vide u različitim spektrima.

Zahvaljujući ovim elementima, dobro obučena osoba će sa samo par pogleda u gotovo svim slučajevima prepoznati da li se radi o originalu ili falsifikatu dokumenta. Kažem „gotovo svim“ jer ima slučajeva korišćenja originalnog pasoša za kriovotvorenje - u Velikoj Britaniji je, recimo, nedavno ukradeno preko 3.000 blanko pasoša. Tada u pomoć mora da se pozove čip.



Slika 52 Proizvodna traka za nove pasoše

5.13 Novi srpski pasoš crven i sa sedam nivoa zaštite

Na koricama pasoša, koje su carsko crvene boje, nalaziće se ime i grb Republike Srbije, natpis „pasoš“, napisan ćirilicom u zlatnoj boji i oznaka da je pasoš biometrijski. Na unutrašnjoj strani korica je natpis „Srbija“, naizmenično ćirilčno i latinično, koji će biti vidljivi samo na UV svetlu.

Prvi list u pasošu je polikarbonatski i tvrdi je u odnosu na druge listove, ostale strane, kojih ima ukupno 32, namenjene su za pečate i vize, i prošivene su na specijalan način i specijalnim koncem koji je fluorescentan.

I druga strana je polikarbonatska, kao na kreditnim karticama, a na prvoj strani srpskim, francuskim i engleskim jezikom napisano je "pasoš". Na toj stranici su lični podaci vlasnika (*fotografija, ime, prezime, mesto i datum rođenja, serijski broj i ostali podaci koje sadrži i sadašnja putna isprava*).

Prema elementima zaštite novi pasoš se najviše razlikuje od starog i ima sedam nivoa zaštite, što ga čini jednim od najmodernijih u Evropi. Novina je nevidljivi čip sa biometrijskim podacima vlasnika. U dnu druge strane nalazi se mašinski čitljiva zona sa ličnim podacima. Zaštita ove stranice je izuzetno važna kako bi se sprečilo falsifikovanje, tako da ima kinegram, optički varijabilne boje, u procesu laminacije unose se mat i sjajni elementi, i napravljena je od više slojeva plastike. Podaci se urezuju laserom, ali ne na prvi, već na donje slojeve polikarbonata. To znači da bi neko, ako hoće da izmeni podatke, morao da ošteti površinski sloj.

I ostale stranice, predviđene za vize, imaju grb Srbije, sadrže i vodeni žig, zaštitne niti i druge skrivene elemente, koji pasoš čuvaju od falsifikovanja.

Pasoši važe deset godina. Na izradi idejnih rešenja za pasoš radila je zajednička komisija MUP-a i Zavod za izradu novčanica.

Dok će građani moći da biraju da li žele da im novoj ličnoj karti bude i čip sa biometrijskim podacima, na pasošu je ovaj detalj - obavezan.

Pored prve i druga strana je polikarbonatska, kao na kreditnim karticama, a na prvoj strani srpskim, francuskim i engleskim jezikom napisano je „pasoš“. Druga stranica sadrži lične podatke vlasnika (*fotografija, ime, prezime, mesto i datum rođenja, serijski broj i ostali podaci koje sadrži i sadašnja isprava*).

Prema elementima zaštite novi pasoš se najviše razlikuje od starog i ima sedam nivoa zaštite što ga čini među najmodernijima u Evropi. U MUP-u tvrde da će novi pasoš Srbije biti jako teško falsifikovati.

Novina je nevidljivi čip sa biometrijskim podacima vlasnika. Dok će građani Srbije, pri izradi novih ličnih karata, moći da biraju da li žele da na dokumentu bude i čip sa biometrijskim podacima, na pasošu je ovaj detalj obavezan.

U dnu strane nalazi se mašinski čitljiva zona sa ličnim podacima.

Zaštita ove stranice je izuzetno važna kako bi se sprečilo falsifikovanje, pa ima kinegram, optički varijabilne boje, u procesu laminacije unose se mat i sjajni elementi, i napravljena je od više slojeva plastike. Podaci se urezuju laserom, ali ne na prvi, već na donje slojeve polikarbonata. To znači da bi neko, ako hoće da izmeni podatke, morao da ošteti površinski sloj.

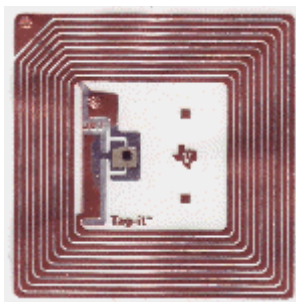
I ostale stranice, predviđene za vize, imaju grb Srbije, sadrže i vodeni žig, zaštitne niti i druge skrivene elemente, koji pasoš čuvaju od falsifikovanja. Pasoši će važiti deset godina.

Na izradi idejnih rešenja za pasoš radila je zajednička komisija MUP-a i Zavod za izradu novčanica.

Preporuka Evropske unije je da njene članice koriste dve boje za ovu putnu ispravu - crvenu ili plavu.

5.13.1

Šta je u čipu



Slika 53 Primer čipa sa antenom

Čip nije kontakti (*kao npr. u elektronskim ličnim kartama*), već se očitava bez kontakta sa čitačem, putem elektromagnetnih talasa. Iako je struktura vrlo slična PKI čipovima koji se koriste za lična dokumenta, zbog okolnosti u kojima se koriste nivo sigurnosti je niži. To je izazivalo velika negodovanja u javnosti, zbog navodne mogućnosti neovlašćenog čitanja sadržaja. Opasnost te vrste je zapravo mala, jer da bi se pristupilo podacima, mora da se pročita MRZ, a zatim da se određenom manipulacijom tih podataka dođe do pristupne šifre za podatke, koja se prosleđuje čipu na proveru. Ovaj način pristupa podacima se zove Basic Access Control (BAC⁴⁰) i prisutan je u gotovo svim do sada izdatim e-pasošima.

Može li neko neprimetno da pročita MRZ pasoša koji je u našem džepu ili torbi? Teško. Čip i njegova antena se, zavisno od proizvođača, nalaze skriveni ili u glavnoj strani (*kao kod nas*) ili u koricama pasoša (*kao u npr. Nemačkoj*). Neke države čak koriste metalizirane folije u koricama, koje sprečavaju svaki pristup čipu kada je pasoš sklopljen, mada to verovatno ima više psihološki nego praktičan značaj. Pojavile su se i tanke metalne kutije za pasoše...

S obzirom da je korišćenje RFID čipova fakat i neizbežno je, kao što je na primer naš pasoš, sve što možemo da uradimo to je da smanjimo rizik od neželjenog očitavanja. Pre

⁴⁰ BAC - Basic Access Control

svega, dokument ne nosimo uvek sa sobom nego samo ako moramo i uvek ga držimo u metalnoj zatvorenoj kutiji, jer ona može da potpuno onemogući očitavanje (*faradejev kavez*).

U samom čipu se nalaze svi tekstualni podaci koje vidimo na glavnoj strani (*ime, prezime, adresa, broj pasoša, jmbg, rok važenja...*), uključujući fotografiju nosioca. Podaci se smeštaju u tzv. Data grupe, a ostavljen je prostor za buduće definicije onoga što će one čuvati, jer se sada ne koriste sve koje su na raspolaganju. Najvažnija stvar je daje snimljeni skup podataka digitalno potpisalo odgovarajuće državno telo, pa se ne može neopaženo izmeniti

Sa pasošima je već sasvim druga priča. Za razliku od ličnih karata u pasoše su ugrađeni čipovi koji se mogu očitati beskontaktnim putem (*RFID*).

To već daje dovoljno prostora za skepsu i zabrinutost, jer beskontaktno očitavanje znači da čip može biti očitao u bilo kom trenutku i bez našeg znanja, jer nije neophodno da pasoš izvadite iz džepa da bi on bio pročitao.

Naravno, ne treba da brinemo za podatke. Sasvim je sigurno da su podaci u čipu bezbedni u smislu da ih niko ne može neovlašćeno očitati, pogotovo bez našeg znanja, pošto verovatno i za njihovo čitanje, kao i za čitanje lične karte, mi moramo da u čitač ukucamo PIN kod i uz uslov da način zaštite nije slab i da nema nekih propusta.

Međutim, problem ipak postoji, jer je očitavanjem čipa moguće pročitati njegov jedinstveni broj, a taj jedinstveni broj se može upotrebiti da nas identifikuje, jer taj broj u našem pasošu je dodeljen našem pasošu, i gde god da ga neko očitao, znaće da se radi o istom pasošu. Sve što je potrebno, to je da se nekako očitani broj poveže sa nama, a to se može uraditi na svakom mestu gde mi i inače moramo da se identifikujemo: na raznim šalterima, prilikom prelaska granice, potvrdom karata na aerodromima i u bilo kojoj drugoj situaciji gde neko može da ima pristup našim ličnim podacima i da istovremeno očitao naš dokument (*sa ili bez našeg znanja*).

Da stvar bude gora, proizvođači čipove isporučuju u serijama, a to praktično znači da je očitavanjem jedinstvenog broja čipa, moguće utvrditi kojoj seriji pripada, a time i koji dokument je očitao, a za pasoš i kojoj državi pripada.

5.13.2

Nije samo pasoš nezgodan

Pasoš nije jedini dokument koji ima RFID čip. RFID tehnologija je već godinama široko rasprostranjena, tako da je moguće da kod sebe imamo neki drugi dokument koji takođe ima ugrađen čip za beskontaktno očitavanje. Na primer, imamo li karticu za identifikaciju prilikom ulaska u neki objekat a koja se očitava beskontaktno (*ne mora biti u obliku kartice, može biti i dugme, privesak za ključ ili nešto drugo*). U njoj je isti čip kao i u pasošu i sve što važi za pasoš, važi i za tu karticu - gde god da postoji RFID čitač on će tu karticu očitati.

Da stvar bude još komplikovanija, svaki RFID čitač čita svaki RFID karticu. Tek kada je očitao, čitač utvrđuje da li je očitana kartica “njegova” pa ako jeste on dalje obrađuje podatke, a ako nije, on očitano karticu zanemaruje. Čak i da proba da pročita podatke iz nepoznate kartice, ne bi uspeo jer podaci u kartici su šifrovani.

To znači da bilo ko ko ima čitač RFID kartica može da očita sve RFID kartice. No, očitavanje se uglavnom svodi na to da se pročita jedinstveni broj kartice, ali drugi podaci su šifrovani i po pravilu bezbedni.

Dosta je teorije, da vidimo šta se može u praksi

Koliko je to izvodljivo u stvarnosti pokazuje eksperiment koji je izveo Kris Pedžet. On je nabavio RFID čitač i povezao ga sa svojim prenosnim računarom, smestio sve u automobil i malo se provozao Sanfranciskom. RFID čitač koji je imao domet od oko 9 metara je za vreme vožnje skenirao RFID kartice na koje je nailazio. U roku od dvadeset minuta očitao je dve kartice, koje je, na osnovu serijskog broja identifikovao kao pasoše.

Ne samo to, nakon toga na Blek Het konferenciji je demonstrirao jednostavan uređaj koji klonira RFID kartice, što će reći, očita jednu RFID karticu i onda drugu, praznu, isprogramira tako da se predstavlja kao originalna kartica.

Neko sa bujnom maštom bi svakako mogao da smisli mali milion načina da se ovako nešto zloupotrebi.

5.13.3

Bezbednije i brže na granicama

Biometrijski podaci na pasošima skraćuje zadržavanje na graničnim prelazima. Već sada u redu za imigrante na aerodromima u Velikoj Britaniji oni koji imaju pasoše koji sadrže sken irisa (*dužica oka*) ne čekaju, već prolaze kontrolu za nekoliko sekundi.

Rasprava o slobodi i humanizmu s jedne i bezbednosti s druge strane pada u vodu kada se pogleda primer Australije. Ne samo da je upotreba e-pasoša povećala sigurnost kod provere putnika i otkrivanja lažnih isprava, pojednostavila i ubrzala proces čekiranja viza i imigracionih dokumenata, već se pokazala odlično i zato što Sidnejski aerodrom nema mogućnost proširenja kapaciteta, a očekuje se da se broj putnika duplira do 2010. godine.

5.14 Identitet u par kilobajta



Nove lične isprave sa čipom izazivaju kontroverzne reakcije domaće javnosti, ali bi tehnološki svesnijim među nama mogle znatno da olakšaju život.

Prošle godine je Ministarstvo unutrašnjih poslova Republike Srbije započelo sa izdavanjem tzv. „elektronskih“ ličnih dokumenata (*ličnih karti i pasoša*). Dokumenti se nazivaju elektronskim zbog toga što u sebi sadrže memorijske čipove u kojima su smešteni tekstualni, biometrijski i drugi podaci. Nove lične isprave omogućice građanima da koriste usluge elektronske uprave i da putuju s pasošem koji je usklađen sa svetskim standardima.

Međutim, izdavanje i korišćenje biometrijskih isprava podrazumeva složenu i skupu infrastrukturu i organizaciju. Ovaj projekat srpski MUP je započeo još 2000. godine, što je bio pionirski poduhvat, jer je tada retko koja zemlja, čak i u svetskim okvirima, razmišljala o nečemu sličnom. Razmotrićemo nešto više detalja o tehničkim i organizacionim preduslovima za izdavanje i korišćenje biometrijskih ličnih isprava od onoga što je u javnosti bilo dostupno.

5.14.1 Prikupljanje podataka

Kao i do sada, izdavanje ličnih isprava obavlja se u policijskim stanicama širom zemlje. Na oko 180 lokacija u svim gradovima i većim mestima Srbije nalazi se 300 sistema za akviziciju podataka. Svaki sistem sastoji se od: savremenog PC računara, skenera za otiske prstiju rezolucije 500 dpi, elektronske table za digitalizaciju potpisa, digitalnog fotoaparata sa rezolucijom 6 do 10 megapiksela, stonog skenera za dokumenta i štampača.

Prikupljeni podaci slivaju se u centralni računar na sigurnoj lokaciji. Zaštita podrazumeva fizičko obezbeđenje, ali, naravno, i tehničku zaštitu (*kriptovanje*) pri prenosu i smeštanju podataka. Uz sistematsko bekapovanje podataka, dodatna mera zaštite integriteta podataka je i to što se isti ti podaci nalaze i u posebnom sistemu za obradu otisaka prstiju.



Slika 54 Detalj iz proizvodnje ličnih karti u Zavodu za izradu novčanica u Beogradu

Centralni računar zapravo je klaster od dva računara IBM System p 570, svaki sa po 16 procesora i 128 GB radne memorije, koji rade pod operativnim sistemom AIX (*IBM-ova verzija UNIX-a*). Na klasteru je postavljeno nekoliko virtuelnih servera koji koriste odgovarajući broj procesora i ostalih resursa, a svim virtuelnim serverima na raspolaganju je više desetina terabajta kapaciteta na hard diskovima.

5.14.2 Otisci prstiju

AFIS u MUP-u Srbije trenutno se sastoji od 90 računara koji se bave obradom otisaka prstiju, od čega je čak dve trećine zaduženo za sušto poređenje otisaka. U sistemu se koriste slike otisaka prstiju i, naravno, slike koje nastaju analizom otisaka i ističu karakteristične linije. Policije širom sveta za arhiviranje i razmenu otisaka koriste standardni format zapisa pod imenom WSQ⁴¹ i takav zapis se, pored ostalog, upisuje na čip lične karte, a i na pasošima.

Srpski AFIS sistem trenutno je dimenzionisan tako da može da smešta i obrađuje podatke o deset miliona osoba. Naravno, i ovaj sistem poseduje sve potrebne mere fizičke i tehničke zaštite.

5.14.3 Softver

Sva računarska oprema MUP-a Srbije nije, naravno, nabavljana u isto vreme, od istog proizvođača i nije jednako tehnički savremena. Pošto su u pitanju stotine računara koji rade pod različitim operativnim sistemima (*UNIX, Linux, Windows...*), koristi se takozvana troslojna softverska arhitektura, gde je middleware sloj Java, što je omogućilo da potrebne aplikacije rade na bilo kojoj platformi. Kao svojevrsna dodatna mera zaštite, kao što je dobro poznato nama koji isprobavamo razne nove verzije softvera, zvanična „politika“ ljudi u MUP-u jeste da se koriste isključivo poslednje stabilne verzije softvera. To se odnosi i na operativne sisteme i na njihova jezgra, kao i na programe za upravljanje bazama (*Oracle, DB2...*), ali i na sav ostali softver.

Ne samo da je upotreba biometrijskih ličnih isprava potreba savremenog sveta, već je to retka oblast u kojoj ne zaostajemo za ostatkom sveta, nego smo, naprotiv, ispred mnogih. U ovom tekstu nisam se bavio pitanjima privatnosti i zloupotrebama prikupljenih podataka o pojedincima. Uostalom, policija i sada ne uzima više podataka o svima nama nego što je to bilo i ranije, već je samo drastično osavremenila svoju aktivnost. Onako „usput“, mi građani dobićemo mogućnost korišćenja elektronskog potpisa, a prednosti toga tek ćemo otkrivati kako se bude razvijala e-uprava u našoj državi.

⁴¹ WSQ - Wavelet Scalar Quantization

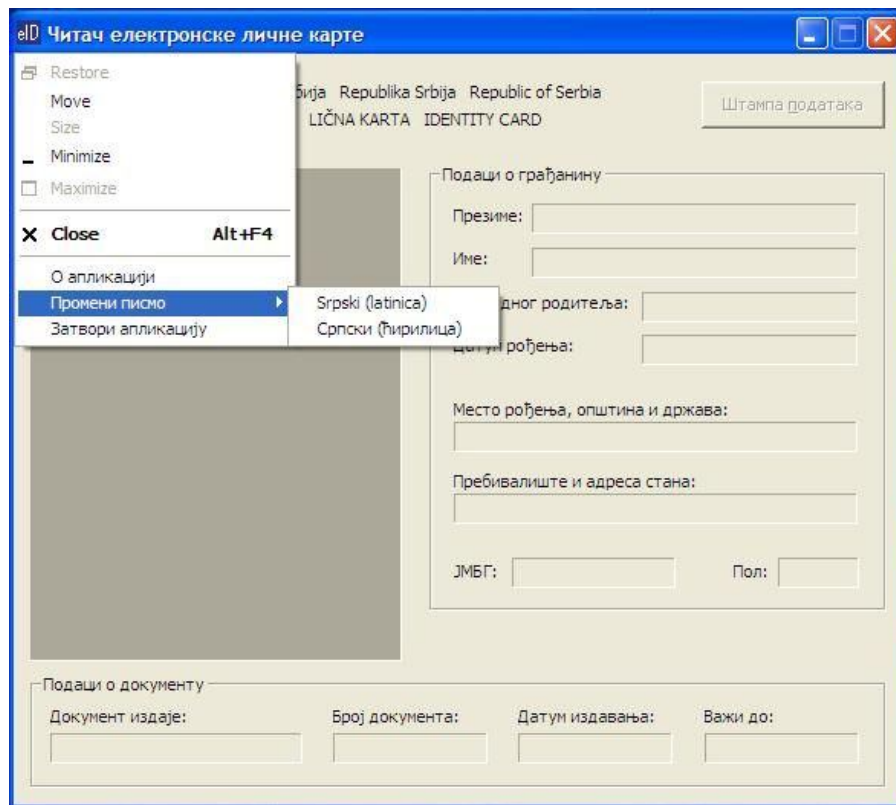
5.15 Čitač elektronske lične karte „ČELIK“

Aplikacija ČELIK (*Čitač Elektronske Lične Karte*) služi za očitavanje čipa elektronske lične karte i prikazivanje javno dostupnih podataka o nosiocu lične karte i dokumentu.

Na sajtu MUP-a mogu se pronaći podaci o aplikaciji „čelik“ koja bi, kako je navedeno, trebalo da radi sa svim čitačima smart kartica koji se mogu kupiti kod prodavaca računarske opreme. Podaci sa lične karte se automatski očitavaju kada se pravilno ubace u čitač, na većini uređaja kartica se ubacuje položena, sa čipom nagore



Slika 55 Način očitavanja čipa elektronske lične karte



Slika 56 Aplikacija ČELIK

5.16 Testiranje putnih isprava (pasoši prolaze kroz „torturu“)



Slika 57 Detalj sa proizvodne trake

Nadomak turističke sezone pojačava se gužva na policijskim šalterima jer građani menjaju stare pasoše za novi biometrijski. Bez obzira na to što mnogi ovo rade u poslednjem trenutku, u ZIN-u⁴² kažu da će na zahtev MUP-a odštampati u roku bilo koju količinu novih pasoša. Nema razloga za sumnju u njihov kvalitet jer pre nego što izađu iz ZIN-a prođu takvu „torturu“ na mašinama da je vlasnik pasoša ne može ni zamisliti.

Ovaj način provere kvaliteta prolazi i polikarbonatna strana pasoša u kojoj se nalazi integrisan čip sa antenom. Ta strana je nosilac biografskog i biometrijskog identiteta građanina, što znači da MUP na njoj, u procesu personalizacije, upisuje vidljive podatke kao što su ime i prezime vlasnika pasoša, a iste te podatke upisuje u čip koji je nosilac tzv. digitalnog identiteta građanina.

Takva polikarbonatna stranica ušiva se u pasošku knjižicu i pre slanja MUP-u, kao kupcu, svaka serija prođe različite mašine, tzv. mučilice koje simuliraju neke postupke koji najčešće dovode do fizičkog oštećenja pasoša tokom njegove upotrebe.

- Jedna mašina simulira nošenje pasoša u zadnjem džepu. Pasoš se stavi u nju, a ona je napravljena tako da podražava džep na pantalonama. Veštačka ruka udara po tom pasošu koji se istovremeno uvija i meškolji kao, kad putnik sedi u automobilu ili avionu a pasoš mu ostao u zadnjem džepu.
- Druga mašina simulira provlačenje pasoša kroz čitač na granici i to oblasti tzv. mašinski čitljive zone koja se nalazi na dnu stranice na kojoj su napisani podaci o vlasniku. Čitač tada prepoznaje određene karaktere kojim stvara ključ i očitava podatke sa čipa. To provlačenje simuliramo zato da ne bi došlo do grebanja ili oštećenja.
- Treća mašina radi tzv. pen test, to jest test neprekidnog pisanja olovkom po stranici pasoša namenjenoj vizama, sa ciljem da se vidi da li će oštetiti čip ili antenu u polikarbonatnoj strani ako koristite tu stranicu kao podmetač da nešto zapišete.
- Četvrta mučilica testira ceo pasoš na uvijanje, kad ga na granici, na primer, nervozno uvijate, ili kad u torbi trpi pritisak zbog kog se uvija.
- Peta - neprekidno simulira udaranje pečata na viznoj strani,
- Šesta - ispituje stabilnost polikarbonatne strane koja je prišivena u pasošu, simulira i otvaranje i zatvaranje pasoša.

⁴² ZIN - Zavodu za izdavanje novčanica

- Sedma mašina ispituje silu čupanja odnosno izdržljivost na mestu gde je ušivena polikarbonatna strana. Zapravo, kolika je sila potrebna da se to iščupa iz pasoša. Neki misle da ako iščupaju polikarbonatnu stranu i ne oštete je prilikom čupanja mogu da je stave u drugi pasoš i tako naprave savršen falsifikat. Zato je poenta da ga ušijemo tako da treba enormna sila za čupanje i da, kad se to uradi, ta stranica bude tako oštećena da ne može biti iskorišćena.



Slika 58 Testiranje neprekidnim pisanjem



Slika 59 Neprekidno otvaranje i zatvaranje

Naša lična karta i biometrijski pasoš prošli su provere i testiranja kod svetski poznatih firmi koje se bave sertifikacijom upravo pasoša i ličnih karata.



Slika 60 Tri hiljade udaraca po pasošu

Kod simulacija nošenja pasoša u džepu, mašina izvede 3.000 udaraca jedan za drugim. Kod simulacije provlačenja kroz čitač na granici - 3.000 puta uzastopno pasoš bude provučen pod valjkom.

Kod simulacija pisanja olovkom po stranici - mašina bez pauze ispisuje jedan sat neprekidno, a po stranici se ispiše desetak metara hemijskom olovkom.

Kod simulacije uvijanja pasoša na unutra i ka spolja mašina ga 3.000 puta uzastopno uvija u obe strane, a druga mašina još 3.000 puta radi uzastopno savijanje. Kad je reč o simulaciji udaranja pečata, mašina obavi 70 uzastopnih udaraca snagom kojom se inače stavlja pečat. Prema pravilniku, mašina mora da odradi i 3000 otvaranja i zatvaranja pasoša na mestu gde se nalazi polikarbonatna strana.

5.17 MUP-u „Zlatni globus“ za uvođenje digitalnih dokumenata

„Zlatni globus“ za najveći IT doprinos, koji su do sada dobijale kompanije za najveći doprinos srpskoj privredi, 2008 godine pripao je Ministarstvu unutrašnjih poslova Republike Srbije, zbog uvođenja digitalnih dokumenata - putnih isprava, a pre svega ličnih karata sa čipom, što će omogućiti punu primenu servisa elektronske Vlade zahvaljujući digitalnom potpisu za građane.



Slika 61 Detalj sa ceremonije

5.18

ZAKLJUČAK

Razvojem i primenom novih, naprednih tehnologija, pre svega tehnologije SMART kartica i biometrijske tehnologije, u utvrđivanju i proveru identiteta lica, dobijamo identifikacioni dokument koji pruža široku osnovu za pouzdanu identifikaciju kako u svakodnevnom životu, tako i u svim oblastima gde su zastupljene elektronske transakcije.

Brzo će doći dan kada će pitanje pouzdanog utvrđivanja identiteta konačno zauzeti drugorazredni značaj, ali ne kao nevažno, već stoga što će taj postupak postati javan i siguran, tako da će krivična dela zloupotrebe identiteta postati prošlost.

Građani će moći da koriste vladine servise, da kupuju proizvode elektronskim putem bez straha od mogućih zloupotreba, putnici će putovati brže i lakše prelaziti granice, preduzeća će biti u prilici da omoguće svojim radnicima obavljanje poslova sa udaljenih mesta, potpuno sigurna da samo oni mogu pristupiti određenim podacima.

Sve to znači razvoj sigurnih i pouzdanih elektronskih transakcija odnosno razvoj usluga e-vlade, e-trgovine, e-poslovanja, e-bankarstva... putem Interneta. Zbog porasta krivičnih dela zloupotrebe identiteta, među donosiocima odluka u vladama i poslovnim organizacijama, sve je manje podeljenih mišljenja u shvatanju važnosti i ozbiljnosti pitanja sigurnog i pouzdanog utvrđivanja identiteta. Identifikacioni dokument baziran na tehnologiji SMART kartica i biometrijskoj tehnologiji, učiniće da svet neizbežno postane mnogo komplikovaniji osobama koje se bave zloupotrebom identiteta.

Dilemu oko zloupotrebe naša država bi trebalo pod hitno da reši: Nema razloga za paniku povodom uvođenja biometrijskih dokumenata. Što se tiče zabrinutih i nezabrinutih, bilo bi dobro kada bi u njihovom odnosu bilo više tolerancije, više nastojanja da se barem poštuju stavovi druge strane. Verujem da će komunikacija naših građana sa državom postati kvalitetnija, jednostavnija i jeftinija, što podrazumeva korišćenje elektronske komunikacije. Takođe očekujem da se ta komunikacija odvija u normativnim i tehničkim uslovima koji su potrebni i podobni da eliminišu ili barem na najmanji stepen svedu mogućnost ugrožavanja prava na zaštitu podataka o ličnosti i svakog drugog ljudskog prava.“

Bilo da je u pitanju terorizam, kriminal, ili potreba da se siromašni i ozlojeđeni sloj drži na oku, hardversko-softverski sistemi za nadzor i indentifikaciju doživljavaju procvat. Kombinujući različita tehnološka rešenja, IT industrija u ovom polju ostvaruje do skoro nezamislive stvari koje smo viđali u filmovima, a može se reći da je sve ovo tek početak.

6

Literatura:

- [1] Radna grupa, „Projekat integrisanog automatizovanog sistema za personalizaciju elektronskih identifikacionih dokumenata“, MUP 2004. godine.
- [2] Radna grupa, „Projekat integrisanog rešenja obezbeđenja i kontrole prelaska državne granice“, 2003. godine.
- [3] Komitet eksperata za terorizam (*CODEXTER*), Grupa specijalista za identifikaciona dokumenta i terorizam (TER-S-IT), Nacrt preporuke o identifikacionim i putnim dokumentima i terorizmu, 2005. godine.
- [4] Zakon o elektronskom potpisu, decembar 2004. godine.
- [5] Radna grupa, „Osnovni koncepti novih elektronskih identifikacionih dokumenata“, MUP, 2004. godine.
- [6] The eEurope SMART Card Čarter, ELECTRONIC IDENTITY WHITE PAPER, 2003.
- [7] SiliconTrust & Infineon Tehnologies, „IDENTIFICATION“, SECURE“, Edition 2/2003.
- [8] W.Rankl & W.Effing, SMART CARD Handbook, 2002.
- [9] The United Kingdom Parliament, House of Commons Hansard Debates, novembar 2003.
- [10] Ferraiolo, D. F., Kuhn D. R., Chandramouli, R., Role-Based Access Control, Artech House, 2003.
- [11] Rankl, W., Effing, W., Smart Card Handbook 3rd ed., Jhon Wiley, 2002.
- [12] Hassler, V., Security Fundamentals for E- Commerce, Artech House, 2000.
- [13] N. K. Ratha, J. H. Connell, R. M. Bolle, „Enhancing security and privacy in biometrics-based authentication systems“, April, 2001.
- [14] „Biometrics The measure of man“, The Economist, 2000
- [15] H. M. Inman, The Emergence of Biometrics, MIS 476 - Indiana State University,
- [16] P. Jonathon Phillips, Alvin Martin, C.L. Wilson, Mark Przybocki, „An Introduction to Evaluating Biometric Systems“, National Institute of Standards and Technology, 2000
- [17] Smart Card Alliance, „Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems“, 2002
- [18] Julian Ashbourn, The Distinction Between Authentication and Identification, 2000.
- [19] TeleTrustT, „Trusted E-Commerce: Idea Becomes Reality“, 2002.

- [20] Marcel Hametner, „It’s all about Identification...“, Secure, January 2002.
- [21] A Smart Card Alliance White Paper, „Secure Personal Identification Systems: Policy, Process and Technology Choices for a Privacy-Sensitive Solution“, February 2002.
- [22] Datastrip, „DSVerify 2D – Portable 2D Bar Code / Biometric Verification Reader“
- [23] International Civil Aviation Organization „Machine Readable Documents“
- [24] Dipl. ing. Mladen Radaković, FAKULTET ORGANIZACIONIH NAUKA, Beograd,
- [25] Dr Dejan Simić, FAKULTET ORGANIZACIONIH NAUKA, Beograd,
- [26] Anthony Cola, „Security Is Not Child’s Play“, Card Technology, 2002.
- [27] Branko Nikitović - PC Pres br.128, decembar 2006
- [28] Branko Nikitović - PC Pres broj 129, januar 2007
- [29] Đorđe Vujičić, dipl. el. ing. - info 3/2008 str.102

Internet:

- [1] Internet prezentacija, <http://www.pkiforum.org/>
- [2] Internet prezentacija, <http://www.aidia-i.ba/>
- [3] Internet prezentacija, <http://www.scmmicro.com/>
- [4] Internet prezentacija, <http://www.verifone.com/>
- [5] Internet prezentacija, <http://www.ramresearch.com/>
- [6] Internet prezentacija, <http://www.mpo.com/>
- [7] Internet prezentacija, www.smartcardbasics.com/
- [8] Internet prezentacija, <http://www.txsystems.com/>
- [9] Internet prezentacija, <http://www.innovonics.com/>
- [10] Internet prezentacija, <http://www.athena-scs.com/>
- [11] Internet prezentacija, <http://www.ietf.org/rfc/rfc2459.txt>
- [12] Internet prezentacija, <http://www.w3.org/Signature>
- [13] Internet prezentacija, <http://xml.apache.org/security/>
- [14] Internet prezentacija, <http://www.zurich.ibm.com/jcop>
- [15] Internet prezentacija, <http://www.cryptoflex.com>
- [16] Internet prezentacija, <http://www.cryptoflex.com/Support/documentation>
- [17] Internet prezentacija, <http://www.ietf.org/rfc/rfc2437.txt>