Vladimir B. Đorđević, dipl.inženjer
vlada@podatak.com

SMART KARTICA

Prokuplje, jun 2009.

Sadržaj:

1. UVOD

Predmet ovog rada je tehnologija rada smart kartica i način na koji se smart kartice primenjuju u zaštiti i čuvanju podataka.

Smart kartica je kartica koja po izgledu dosta podseća na običnu kreditnu ili debitnu karticu; ono što je odvaja od obične kreditne kartice je integrisano kolo ili čip na kome se nalaze procesor i memorija (RAM i ROM) i delovi koji omogućavaju komunikaciju odnosno razmenu podataka sa okolinom. Čip smart kartice je ono što ove kartice čini „pametnim karticama“ (smart kartica = pametna kartica). Smart kartica kao takva predstavlja veoma pogodan alat za čuvanje podataka i obezbeđivanje sigurnosti istih. Obezbeđivanje sigurnosti podataka označava da se treba odbraniti od neprijatelja, a da bi se to izvelo treba neprijatelja prvo definisati tj. treba utvrditi šta utiče na bezbednost podataka koji nose informacije kao i koji su to oblici ugrožavanja informacija.

Kako bi zaštitili smart karticu odnosno podatak/podatke na njoj, trebalo bi prvo dobro utvrditi samu strukturu i tehničke karakteristike smart kartice kako bi znali šta treba i na koji način štititi. Iz tog razloga treba izložiti istoriju, osobine, tipove i karakteristike smart kartica kao i standarde koje moraju zadovoljiti što je prikazano u prvom delu rada.

Takođe, da bi smo znali kako zaštititi jednu smart karticu trebalo bi da znamo od čega istu štitimo tj. koji su problemi vezani za bezbednost informacija, pretnje u vezi sa bezbednošću kao i zahtevi za zaštitu informacija. Pametna kartica obezbeđuje različite opcije nivoa sigurnosti koje idu od jednostavnih kontrola pristupa pa sve do zaštite složenih sistema primenom različitih algoritama za šifrovanje i posebnih vidova komunikacije između korisnika takvog jednog sistema. U tom smislu treba ponuditi tehnička rešenja, odnosno navesti kriptološke metode i način primene u zaštiti što je prikazano u drugom delu rada.

Na osnovu ovog rada će se takođe videti kako su se pametne kartice pokazale kao veoma pogodan medijum za obavljanje različitih transakcija, autorizaciju i identifikaciju. Kako se sposobnosti inteligentnih kartica povećavaju iz dana u dan polako se dolazi u takvu situaciju da se pametne kartice mogu koristiti u više namena počev od zamene za novčanik tj. novac pa preko vozačkih dozvola i različitih propusnica sve do zamene za kompletan zdravstveni karton, a sadržući različite sertifikate, smart kartice možemo koristiti za identifikaciju u bilo koje vreme i na bilo kom mestu.

2. ISTORIJA SMART KARTICA

Koreni današnjih smart kartica sežu u 1950. godinu do Diners kluba koji je proizveo prvu plastičnu karticu i počeo da je koristi kao sredstvo plaćanja. Za razliku od prethodne kartice koja je napravljena od papira za proizvodnju ove kartice je korišćen sintetički PVC material na osnovu koga je nastala ova izdržljiva kartica. Ta prva kartica je, pored toga što se koristila kao sredstvo za plaćanje, takođe i identifikovala vlasnika kao člana određene grupe i bila prihvaćena od strane nekih hotela i restorana. Tada se na tržištu pojavljuju VISA i MasterCard, ali je zbog neovlašćenog mešanja potreba trgovca i banaka bilo potrebno napraviti karticu koja bi se čitala uz pomoć nekog uređaja. Tako se pojavila kartica sa magnetnom trakom koja je omogućila digitalizaciju podataka. Međutim, kako se uz pomoć određenih uređaja moglo pristupiti ovoj kartici i vršiti upisivanje, čitanje i brisanje podataka bilo je potrebno doraditi karticu dodavanjem centralne pozadinkse infrastructure za potvrdu (verifikaciju) i obradu. Ova kartica je bila u velikoj upotrebi u Americi, ali ne i u Evropi. Jedno rešenje je trebalo da bude pojačavanje serverske strane, a drugo rešenje da se osnaži klijentska strana na taj način što bi se prebacio deo aktivnosti sa servera na klijenta. Evropske zemlje su bile pri stavu da je bolje izvršiti pojačavanje klijentske strane i na taj način je u upotrebu uvedena kartica sa integrisanim kolom (Integrated Circuit Card – ICC).

Nemački raketni naučnik Helmut Gröttrup sa svojim kolegom Jürgen Dethloff je 1968. godine podneo patent za kartice sa integrisanim kolom koji je konačno odobren 1982. godine. Slični projekti su usledili i u Japanu 1970. godine kao i u Francuskoj 1974. godine. Prvu probnu upotrebu ovih kartica je uveo Francuski telekom 1983. godine, a upotreba ovih integrisanih kartica u francuskom telefonima je do 1986. godine dostigao višemilionsku upotrebu da bi do 1990. godine dostigao broj od oko 60 miliona korisnika, a do 1996. godine u upotrebi je bilo oko 150 miliona ovih kartica.

Sledeća upotreba je bila u francuskim debitnim karticama “Carte Bleue” 1992. godine. Princip plaćanja uz pomoć “Carte Bleue” je taj što se kartica unosila u mehanizam za čitanje posle čega bi se unosio PIN, a zatim nakon ispravno unetog PINa vršila transakcija. Samo se manji broj transakcija (poput plaćanja putarine na autoputevima) mogao izvršiti bez unošenja PIN-a.

Veliki bum smart kartice doživljavaju tokom 90ih pojavom SIM kartica zasnovanim na tehnologiji smart kartica i njihovom upotrebom u GSM telefonskoj opremi u Evropi. Sa pojavom mobilnih telefona u Evropi upotreba smart kartica postaje učestala.

Naredni stupanj u istoriji smart kartica jeste dogovor MasterCard–a , VISA i Europay-a 1993.godine o zajedničkoj saradnji u kreiranju standarda o upotrebi smart kartica pri plaćanju bilo da se radi o debitnim ili kreditnim karticama. Prva verzija EMV sistema (**E**uropay, **M**asterCard, **V**ISA) je realizovana 1994. godine, a prva stabilna verzija 1998. godine.

3. STANDARDI KARTICA

Svojim standardom 7810:2003 međunarodna ogranizacija je definisala fizičke karakteristike indentifikacione kartice. Standard 7810 definiše četiri veličine kartica[1]: ID-1, ID-2, ID-3 i ID-000.

Format	Dimenzije
ID-1	85.60 x 53.98 mm
ID-2	105 x 74mm
ID-3	125 x 88mm
ID-000	25 x 15 mm

Tabela 1. Veličina kartica

ID-1 fornat kartica definiše veličinu kartica od 85.60 x 53.98 mm, odnosno 3.370 x 2.125 inča. Proporcija strana ovih kartica je 1.5858:1. Ovaj format se najčešće upotrebljava pri izradi bankovnih kartica (kreditnih kartica, debitnih kartica itd.). Ovaj format kartica se danas takođe upotrebljava pri kreiranju vozačkih dozvola u mnogim zemljama (SAD, Kanada, Australia, Novi Zeland, Norveška, i zemlje Evropske Unije). ID-1 format kartica se recimo u Švajcarskoj, Čileu, Peruu i Pakistanu koristi kao standard za izradu ličnih karata i kao veoma čest format prilikom izrade poslovnih – vizit karti. Takođe, ovaj format kartica se recimo u Americi koristi kao format pri izradi pasoša.

ID-2 je format kartica koji definiše dimenzije od 105 x 74mm (4.134 x 2.913 inča). ID-2 je format koji se koristi kod nemačkih identifikacionih dokumenata i koji će se koristiti do novembra 2010. godine kada će se preći na korišćenje ID-1 formata.

ID-3 format kartica je format koji definiše dimenzije od 125 x 88mm (4.134 x 2.913 inča). Ovaj format se koristi širom sveta za pasoše i vize.

ID-000 format definiše veličinu od 25 x 15mm i to je format koji se koristi kod SIM kartica.

ID-1 standardi:

ISO/IEC 7813 definiše fizičke osobine (veličinu, oblik, položaj magnetne trake) i strukturu podataka magnetne trake bankarskih kartica. Po ovom standardu debljina kartica mora da iznosi 0.76mm dok su uglovi kartice zaobljeni sa radijusom od 3.18 mm.[2]

ISO/IEC 7811 je set od 9 standarda (7981-1 do 7981-9) koji koji opisuje tehnike upisa na ID-1 kartici.[3]

[1] http://en.wikipedia.org/wiki/ISO/IEC_7810
[2] http://en.wikipedia.org/wiki/ISO/IEC_7813
[3] http://en.wikipedia.org/wiki/ISO/IEC_7811

ISO/IEC 7816 je internacionalni standart koji se odnosi na elektronsku identifikaciju kartica sa kontaktom pri čemu se pre svega misli na smart kartice. Ovaj standard je uređen od strane internacionalne organizacije za standarde – ISO (International Organization for Standardization) i internacionalne elektrotehničke komisije – IEC (International Electrotechnical Commission).[4]

Delovi ISO/IEC 7816 standarda:[5]

7816 – 1 : Fizičke karakteristike. Ovaj standard je kreiran 1987 godine, dopunjen 1998 a izmenjen 2003.godine. On definiše fizičke karakteristike kartice kao što su dimenzije, elektromagnetno zračenje, lokaciju na magnetnoj traci, otpornost na statički elektricitet.

7816 – 2 : Kartice sa kontaktom – dimenzije i lokacije kontakta. Ovaj standard je kreiran 1988. godine, dopunjen 1999. godine i izmenjen 2004. godine. Standard definiše namenu, lokaciju i električna svojstva metalnih kontanata na kartici.

7816 – 3 : Elektronski interfejs i transmisija protokola. Standard kreiran 1989.godine, dopunjen 1997.godine i izmenjen 2002. i kasnije 2006.godine. 7816 – 3 je dizajniran da se bavi elektronskim signalima i transmisijom protokola. On specificira trenutno i naponske zahteve za električne kontakte:

- Asinhroni poludupleksni, prenos bajt po bajt (T=0)
- Asinhroni poludupleksni, prenos paketa (T=1). Smart kartice koje koriste vlasnički prenosni protokol nose njegovu oznaku.
- T=14 koji uključuje selekcije tipova protokola

7816 – 4 : Organizacija, bezbednost i komande za razmenu. Standard kreiran 1995. godine i dopunjen 2005. godine. Ovaj standard definiše osnovne naredbe za čitanje, pisanje i ažuriranje podataka na kartici.

7816 – 5 : Registracija aplikacionih identifikatora. Kreiran 1995. godine i dopunjen 2004. godine. On definiše aplikacionu identifikaciju koja ima dva dela:

- Registrovani aplikacioni idektifikator dobavljača (RID) koji se sastoji od 5 bajta.
- Polje varijabilne dužine do 11 bajta koje RID može koristiti za identifikaciju specifične aplikacije.

7816 – 6 : Elementi podataka za razmenu. Standard kreiran 1996.godine i dopunjen 2004.godine. Ovaj standard definiše fizički prenos uređaja i operativnih podataka. U njemu su uključena dva prenosna protokola: poludupleksni, prenos bajt po bajt T=0 i poludupleksni,

[4] http://en.wikipedia.org/wiki/ISO/IEC_7816
[5] http://www.tech-faq.com/iso-7816.shtml

prenos paketa T=1. Kartice podržavaju oba protokola, ali ih ne podržavaju istovremeno. Ukoliko se kartica ne pridržava ničega od standarda onda se ona karakteriše kao T=14.

7816 – 7 : Komande za SCQL (Structured Card Query Language). Kreiran 1999. godine. Standard za održavanje i vršenje upita nad bazama, a takođe daje i format definicijama.

7816 – 8 : Komande za sigurnost operacije, Kreiran 1995. godine i dopunjen 2004. godine. Komande za sigurnost operacija su standardizovane ovim kriterijumom. Ovaj standard uključuje komande za unutrašnju bezbednost upravljanja karticom i može da uključi kodirane tehnike i druge bezbednosne metode upravljanja.

7816 – 9 : Komande za organizaciju kartice. Kreiran 1995. godine i dopunjen 2004. godine. Ovaj standard definiše specifikacije za komande za upravljanje karticama. Primarni interes ovog standarda je:

- Opis i kodiranje bezbednosnih atributa povezanih objekata u kartici,
- Funkcije i sintakse drugih komandi,
- Opis i kodiranje životnog ciklusa kartice i srodnih objekata,
- Podaci elemenata u vezi sa ovim komandama,
- Mehanizam za iniciranje poruka izazvanih karticom.

7816 – 10 : Rešavanje električnih signala i reset signala na sinhronim karticama. Kreiran 1999. godine. Ovaj standard uključuje sledeće:

- Strukturu signala
- Snagu
- Strukturu za resetovanje signala koji se šalje između kartice i interfejs uređaja kao što je na primer terminal.

7816 – 11 : Lična identifikacija biometričnim metodama. Kreiran 2004. godine. Ovaj standard je namenjen za ličnu identifikaciju korisnika. Može da koristi biometrijske metode i standarde kako bi postigao ličnu identifikaciju.

7816 – 12 : Kartice sa kontaktom – USB elektronski interfejs i operacione procedure. Kreiran 2005.godine. Ovaj standard definiše operativne uslove integrisanog sklopa kartice koju daje USB interfejsu. integrisani sklop kartica sa USB interfejsom se zove USB-ICC

7816 – 13 : Komande za organizaciju aplikacija i multiaplikacionu okolinu. Od 2006. godine u fazi razvoja.

7816 – 15 : Kriptografske informacione aplikacije. Kreiran 2004. godine. On definiše aplikacije kartice. Ova aplikacija sadrži podatke o kriptografskoj funkcionalnosti. Takođe, ovaj standard definiše zajedničke sintakse i formate za kriptografske informacije i mehanizme za deljenje ovih informacija gde god je to potrebno.

4. TIPOVI ID-1 KARTICA

4.1.Embossed (Kartica sa ispupcenjima)

Kartice sa ispupčenjima su kartice kojima ispupčenja omogućavaju da se tekstualne informacije koje se na njima nalaze budu prebačene na papir uz pomoć korišćenja jednostavnih uređaja. Veličina, forma, visina i poziciju ispupčenja definiše ISO 7811 standard. Jednostavnost ovog sistema ga je učinila široko rasprostranjenim.

4.2.Magnetne kartice

Magnetna kartice predstavljaju tipove kartica kod kojih se podaci upisuju na taj način što se modifikuje magnetni deo. Ono što čini prednost magnetnih traka u odnosu na kartice sa ispupčenjima je smanjenje papirne dokumentacije. ISO 7811-2, ISO 7811-4 i ISO 7811-5 standardi definišu karakteristike magnetne trake, tehniku kodovanja i pozicije. Magnetne kartice imaju kapacitet od 1000 bita.

4.3.Memorijske kartice

Memorijske kartice su kartice koje u sebi imaju EEPROM i ROM memoriju, kao i određenu adresu i logiku vezanu za bezbednost. Kod najjednostavnijih primera logika postoji da spreči upisivanje i brisanje podataka. Složeniji dizajn nam omogućava da se ograniči mogućnost čitanja memorije.

4.4.Inteligentne (Smart) kartice

Pod inteligentnim karticama podrazumevamo kartice koje imaju integrisano kolo. Te kartice spadaju u kartice veličine ID-1 i zasnovane su na ISO 7816 standardu. Ove kartice imaju veću mogućnost čuvanja podataka. Ono što je najvažnije je da se podaci za čuvanje kod ovih kartica mogu zaštititi od neovlašćenog pristupa, menjanja i ugrožavanja. Prednost ovih kartica u odnosu na druge je njihova pouzdanost i duži vek trajanja.

Dakle, inteligentna kartica je plastična kartica na kojoj se nalazi ugrađeni čip i koja skladišti i prenosi podatke između korisnika. Podaci koji se obrađuju ili skladište i obrađuju unutar čipa na kartici ili se čuvaju u memoriji. Svi ti podaci se prenose preko čitača kao osnovnog dela računarskog sistema. Danas je zbog ključnih aplikacija u koje spadaju i zdravstvena zaštita, bankarstvo, transport i preduzetništvo, ovaj sistem inteligentnih kartica u širokoj upotrebi.

5. TIPOVI SMART KARTICA

5.1. Kontaktne Smart kartice

Kod ovih kartica je sva mikroelektronika ugrađena u unutrašnjost kartice u obliku jedno čipa veličine oko 10mm kod koga se na površini nalaze zlatni kontakti. Kontakti omogućavaju da se uspostavi veza sa spoljašnjom jedinicom (Smart Card Reader) što omogućava da neki uređaj uspostavi komunikaciju i prenese energiju u čipu. Kontaktna smart kartica ima 8 kontakata; dva za napajanje, jedan za signal takta, jedan za reset, dva za komunikaciju i dva unapred rezervisana koja se ne koriste. Mnoge kartice pored ovoga imaju na poleđini i magnetnu traku radi kompatibilnosti sa opremom. Kako integrisanom kolu treba napajanje, signal takta koji upravlja procesorom i vezu sa koje će primiti odnosno slati podatke ova kartica to postiže preko kontakata.

5.2. Bezkontaktne Smart kartice

Bezkontaktne smart kartice imaju neku vrstu antene i umesto kontaktne veze koriste neku vrstu elektromagnetskog povezivanja. Međutim, kako prenos energije pada sa udaljenosti, da bi obavila svoju funkciju kartica mora da se nađe u blizini čitača na razdaljinmi od otprilike 3cm. Kao prenos energije i podataka na kartici se koristi induktivna ili kapacitivna veza; signal takta može biti interno izveden, a ulazno/izlazna komunikacija može da se ostvari pomoću jedne od vrsta modulacija.

5.3. Kombinovane kartice

Kombionovane kartice predstavljaju kombinaciju kontaktnih i bezkontaktnih kartica pa se uz pomoć njih može ostvariti to da budu primenljive na bilo koji sistem. Ove kartice kao dodatak imaju i magnetnu traku sa strane kao i dvodimenzionalni ili jednodimenzionalni bar-kod, pa je iz tog razloga kartica multifunkcijska i primenljiva na sisteme.

5.4. Super smart kartice

Dosadašnji tipovi smart kartica su predstavljali pasivne tipove kartica koje su zahtevale spoljašnje izvore napajanja i terminal koji je vršio upis i ispis podataka. Ova ograničenja su uticala na primenu kartica u određenim aplikacijama na taj način što bi npr. svaki pasivni sistem smart kartica morao da osigura raspoloživost terminala u planiranom području primene. Sve ovo je dovelo do toga da se razvije treća generacija smart kartica poznatih pod nazivom super smart kartice. Super smart kartice sadrže tastaturu i LCD displej na površini kartice i kao takve mogu biti potpuno samostalna jedinica ili se opet mogu priključiti na računar (ima površinske kontakte koji joj to omogućavaju).

Mana ovakvih kartica u odnosu na druge kartice je visoka cena proizvodnje, problemi koji se javljaju prilikom pokušaja da se zadovolje ISO standardi kao i relativno mala veličina tastature.

Prednost ovih kartica je mogućnost offline rada i samoprovere. Za razliku od pasivnih kartica koje zavise od terminala, super smart kartice se mogu koristiti na bilo kom mestu i u bilo koje vreme.

6. ELEMENTI SMART KARTICA

Kao i svi ostali računarski sistemi i smart kartica se sastoji od tri elemenata i to od procesorkse snage, čuvanja podataka i sredstvima za učitavanja i izčitavanja podataka. Kod smart kartice procesorsku snagu uglavnom predstavlja mikroprocesorski čip dok je za čuvanje podataka zadužen memorijski čip (EEPROM, FLASH, ROM, RAM). Kod većine smart kartica se ovi resursi kombinuju u jedan čip. Što se tiče prenosa podataka, on se od kartice do kartice menja u zavisnosti od namene. Kako bi kartica mogla da radi ona mora da ima izvor napajanja što uglavnom predstavlja čitač kartica ili se pak taj izvor napajanja nalazi na kartici.

6.1.Mikroprocesor

Mikroprocesor je pametni deo smart kartice koji manipuliše podacima i vrši njihovu interpretaciju. Softver koji se bavi interpretacijom i manipulacijom podataka se ili upisuje u memoriju prilikom proizvodnje kartice ili se naknadno upisujue pod kontrolom mikroprocesora. Mikroprocesori koji se nalaze na smart karticama mogu biti 16-bitni i mogu raditi na taktu od 10 MHz.

6.2.Memorija

Memorija smart kartica može biti ili promenljivog karaktera pri čemu zadržava podatke nakon nestanka napajanja ili promenljiva kod koje podaci nestaju nakon nestanka napajanja, pri čemu bi bilo potrebno da kartica ima bateriju za napajanje. Memorija može takođe biti tipa da dozvoljava i čitanje i pisanje u nju (RAM) ili da dozvoljava samo čitanje iz nje (ROM). Kod većine smart kartica aplikacije zahtevaju memoriju nepromenjivog tipa koja služi za čuvanje podataka o identitetu vlasnika kartice i memoriju promenljivog tipa koja služi za čuvanje podataka promenljivog tipa kao što su recimo stanje na bankovnom ralunu nakon neke transakcije i sl. U tom smislu, memorije na smart kartici se mogu podeliti u tri kategorije: ROM, RAM i PROM. ROM memorija je memorija koja je nepromenljivog tipa i predstavlja memoriju u kojoj su smešteni podaci prilikom proizvodnje. Kod ove memorije se jednom upisan sadržaj ne može menjati. Za razliku od ROM memorije RAM memorije su promenljive i služe za privremeno čuvanje podataka tj. kod tih memorija se podaci čuvaju samo privremeno, odnosno, podaci se nakon nestanka struje brišu. Što se tiče PROM memorije postoje dve vrste te memorije: EPROM i EEPROM. Razlika između EPROM i EEPROM memorije je ta što se EEPROM memorija može reprogramirati, ali je struktura memorije složenija što je čini mnogo skupljom. Memorija može da bude struktuirana na taj način da omogućava različite nivoe zone sigurnosti (otvorena i zatvorena zona). Otvorena zona sadrži podatke koji nisu poverljivi poput podataka o identitetu kartica dok zatvorena ili tajna zona sadrži podatke tipa PIN koda i nedostupna je svima osim procesoru koji proverava broj koji unosi korisnik. Na ovaj način poverljivi podaci nikada ne izlaze sa kartice.

6.3.Ulaz/izlaz

Postoji više načina da se podaci prenesu sa ili iz kartice. Kontaktne kartice obično sadrže metalne kontakte na površini koji služe da kada su ubačeni u čitač budu most tj. povezuju unutrašnjost smart kartice sa spoljašnjim svetom. Bezkontaktne kartice koriste neku od bežičnih tehnologija za prenos podataka što dovodi do uslova da se kartica mora nalaziti u blizini uređaja koji vrši učitavanja odnosno iščitavanja podataka. Super smart kartice imaju na sebi tastaturicu i mali displej i nije im potreban neki uređaj za prenos podataka, već se ti podaci mogu uneti od strane korisnika. Ovakve kartice imaju kontakte koji koriste za komunikaciju sa uređajima takvog tipa.

6.4.Izvori napajanja

Postoje tri metoda napajanja smart kartica:

Preko kontakta iz spoljašnjeg izvora

Kod ovog metoda se energija kartici šalje preko dva kontakta (koja se nalaze na površini kartice) kada se kartica ubaci u uređaj posle čega se vrši pisanje/čitanje podataka. Posle ubacivanja kartice u uređaj, kartica će se sama resetovati (reset on power) i počeće da izvršava program u memoriji koji će početi da komunicira.

Iz spoljašnjeg izvora napajanje prenosom energije

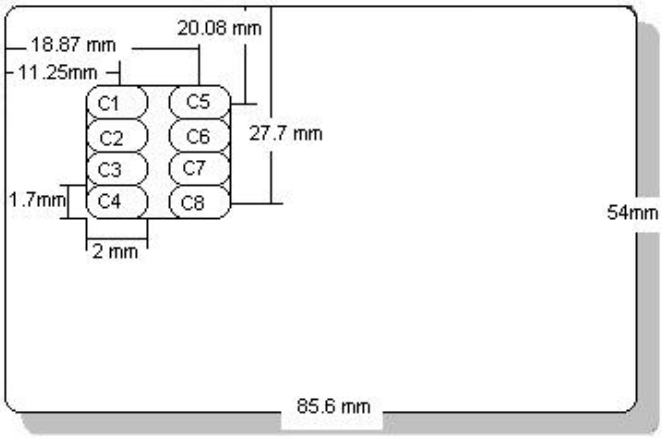
Kod ovog metoda će se bežičnim putem preneti energija koja je dovoljna da u kartici probudi nekakav proces koji će da izvrši neku kratku operaciju, a zatim se ugasi. Kako bi ovo moglo da se omogući kartica mora da se nalazi u neposrednoj blizini tog uređaja kako bi prenos energije imao smisla.

Iz baterije ugrađene u karticu

Kod ovog metoda je baterija sastavni deo kartice i kartica se napaja iz nje. Ova metoda nije baš popularna zbog teškoća koje nastaju zbog zadovoljavanja ISO standarda, a odnose se na dimenzije, težine i troškove koji rastu sa ugrađivanjem baterije u karticu.

7. FIZIČKE i ELEKTRIČNE KARAKTERISTIKE SMART KARTICA

Fizička struktura smart kartice je definisana ISO standardom 7810 i dizajnirana kao ID-1. Dimenzije kartice su 85.6 x 54 mm sa ivicama prečnika 3.18mm i debljinom od 0.76mm. U vreme kada je definisan standard 7810 se nije vodilo računa o tome gde se nalazi čip na ovoj kartici već se vodilo računa o položaju ispupčenja, o položaju magnetne trake i sl. ISO standardom 7816-2 je definisan položaj čipa na smart kartici.

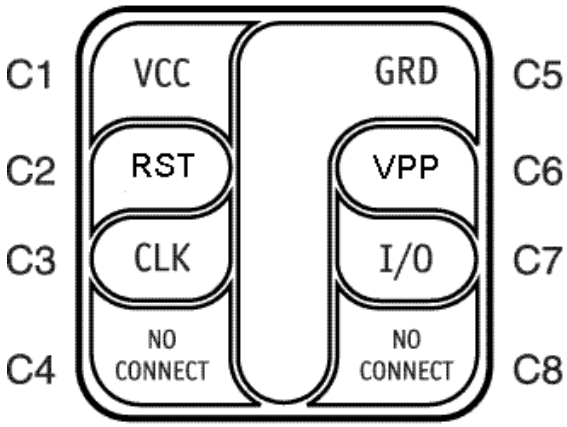


Slik1 broj 1. Dimenzije inteligentne kartice

Intregrisano kolo i čipovi su sastavni deo kartice. Kontakti na kartici su takođe propisani ISO standardom i predstavljaju 5-opinsku vezu sa napajanjem i podacima. Ono što smart karticu čini pametnom jeste integrisano kolo. Integrisano kolo se sastoji od mikroprocesora, radne memorije (RAM), ROM memorije i električki izbrisive programabilne ROM memorije (EEPROM). EEPROM momorija pamti svoje podatke i kada nestane napajanja. Čip koji se nalazi na kartici napravljen je od silicijuma i kao takav je lako lomljiv. Kako se ne bi desilo da se čip prilikom savijanja polomi njegova veličina je svedena na svega nekoliko milimetara.

Veličina, debljina i fleksibilnost su dizajnirani na taj način da zaštite karticu od fizičkog oštećenja. Međutim, to sa druge strane ograničava veličinu memorije i procesorskih resursa koji su na njoj. Ova ograničenja zahtevaju uređaje koji se nalaze van kartice kao npr. napajanje, podaci o vremenu i datumu i dr. koji se nalaze npr. u čitaču. Ova ograničenja mogu degradirati stupanj sigurnosti, jer su zbog toga ti spoljašnji uređaja uglavnom podložni napadima od strane uljeza.

Električne osobine smart kartica su definisane ISO/IEC standardima 7816-2 i 7816-3 i GSM 11.11. inteligentne kartice imaju najčešće osam kontaktnih polja od kojih su dva rezervisana za buduću upotrebu, pa iz tog razloga neki proizvođači proizvode kartice sa samo šest kontaktnih polja. Električni kontakti su obično poređani od vrha naniže sa leva na desno i označeni su sa C1 do C8 što se može videti na slici broj 2.



Slika broj 2. – Kontakti na čipu

Kontakti na čipu:

- VCC – napajanje unosa
- RST – ili se koristi samostalno (reset signal se dobija od interfejsa uređaja) ili u kombinaciji sa internom kontrolom reseta (opciono korišćenje od strane kartice). Ukoliko se sprovodi interni reset snabdevanje naponom iz VCC je obavezno.
- CLK – signal takta
- GND – uzemljenje
- VPP – deo za programiranje ulaznog napona
- I/0 – ulaz ili izlaz za serijske podatke do integrisanog kola unutar kartice

8. PRENOS PODATAKA

Celokupna komunikacija od kartice i prema kartici se odvija preko kontakta C7 (možemo ga videti na slici broj 2). To što se celokupna komunikacija obavlja samo preko C7 označava to da se u jednom trenutku može postići samo komunikacija od kartice prema terminalu, odnosno, komunikacija od terminala prema kartici. Ova komunikacija se zove poludupleksni prenos. Kako je komunikacija između terminala i kartice inicirana od strane terminala odnos o kome je ovde reč je klijent – server odnos.

Pošto se kartica ubaci u terminal, njeno napajanje dolazi od terminala, dolazi do izvršavanja power–on–reset i šalje se odgovor na reset (ATR) ka terminalu. ATR se raščlanjuje, različiti parametri se izvlače iz njega i tada terminal podnosi inicijalnu instrukciju prema kartici. Kartica generiše odgovor i šalje ga nazad terminalu. Klijent – server odnos nastavlja dalje na ovaj način dok se obrada ne završi i kartica izvuče iz terminala.

Sloj fizičkog prenosa podataka definisan je ISO 7816 – 3 standardom koji definiše nivo napona koji se završava prevođenjem u bite 0 i 1.

Postoji više protokola koji služe za razmenu informacija u klijent – server strukturi podataka:

Protokoli	Opis protokola
T= 0	Asinhroni, poludupleksni, prenos bajt po bajt (ISO 7816 – 3)
T= 1	Asinhroni, poludupleksni, prenos paketa (ISO 7816 – 3)
T= 2	Asinhroni, dupleksni, prenos paketa (ISO 7816 – 4)
T= 3	Dupleksni, još nije definisan
T= 4	Asinhroni, poludupleksni, prenos bajt po bajt (proširenje od T=0)
T= 5 do T= 13	Rezervisani za buduću upotrebu
T= 14	Za nacionalne funkcije, nije ISO standard
T= 15	Rezervisan za bzdzću upotrebu

Tabela broj 2. Protokoli za razmenu podataka u klijent – server

Najčešće korišćeni protokoli su T=0 i T=1. Najpopularniji je T=0. Kratak pregled instrukcija ovog protokola je dat na slici broj 3.

Slika broj 3. Tipična T=0 instrukcija

9. SET iNSTRUKCIJA

Postoje četri međunarodna standarda koja definišu tipičan set instrukcija inteligentnih kartica. Preko 50 instrukcija i njihovih izvršnih parametara se definišu ovim standardima. iako se radi o različitim standardima, instrukcije su u mnogome kompatibilne. Standardi o kojima je reč su GSM 11.11 (prETS 300608), EN 726-3, ISO/IEC 7816-4 i CEN standard prEN 1546. instrukcije se klasifikuju po funkcijama:

Selekcija datoteke	Upisivanje i čitanje iz datoteka
Traženje datoteke	Operacije sa datotekama
Identifikacija	Autentifikacija
Kriptografske funkcije	Upravljanje datotekama
Instrukcije za elektronsku kupovinu ili kreditne kartice	Testiranje hardvera
Posebne instrukcije za specifične aplikacije	Podrška protokolu za prenos

Tabela broj 3. Primer tipova instrukcija

Naravno, inteligentna kartica će koristiti samo podskup mogućih instrukcija potrebnih za datu aplikaciju. Ovo je posledica ograničenja vezanih za korišćenje memorije i troškove.

10.OPERATIVNI SISTEM

Iako operativni sistem za procesore smart kartica sadrži nekoliko hiljada bajtova programskog koda on mora obaviti takve zadatke kao što su:

- Prenos podataka preko dvostranog serijskog terminalnog interfejsa,
- Učitavanje operacija nad i upravljanje aplikacijama,
- Izvršna kontrola i obrada instrukcija,
- Zaštićen pristup podacima, upravljanje memorijom,
- Upravljanje datotekama,
- Upravljanje i izvršavanje kriptografskih algoritama.

Za razliku od operativnih sistema poput sistema UNIX, DOS i Windows operativni sistemi za inteligentne kartice nisu prioritetno orijentisani na korisničke interfejse ili sposobnost da pristupe spoljnim periferijama ili medijima za čuvanje podataka. Veličina je obično između 3 i 24 kilobajta. Niža granica se koristi za specijalizovane primene dok je gornji limit vezan za operativne sisteme u slučaju višestruke primene inteligentnih kartica. Pošto je memorijski prostor smart kartica ograničen ne mogu se implementirati sve standardizovane instrukcije i strukture datoteka u sve operativne sisteme za inteligentne kartice. Iz ovog razloga je došlo do uvođenja takozvanih profila u upotrebu standardima ISO 7816 – 4 i en 726 – 3. Profilom se definiše minimum zahteva potrebnih za strukturu podataka i komande.

11. VRSTE NAPADA

11.1. Logički napadi

Logički napadi su napadi koji se dešavaju kada inteligentna kartica radi u normalnim uslovima, ali kada dolazi do osetljivih informacija na taj način što ispituje bajtove koji dolaze i odlaze sa smart kartice. Primer ovog napada je takozvani vremenski napad (timing atack) kod koga se kartici uz pomoć privatnog ključa šalju različiti uzorci bajtova. Informacije koje se dobijaju na osnovu broja nula i jedinica u ulaznom bajtu kao i vreme da se izvrši operacia služe kako bi se eventualno došlo do tajnog ključa. Protivmere za ove napade postoje ali ih veći deo proizvođača smart kartica na sprovodi u delo. Inače, ovakav napad zahteva poznavanje PIN koda kartice, tako da mnoge operacije koje su vezane za tajni ključ mogu biti izvršene na odabranim ulaznim bajtovima.

11.2. Fizički napadi

Fizički napadi su napadi koji se izvode na taj način što se menjaju fizički uslovi poput temperature, frekfencije, napona i sl. Kako bi se pristupilo informacijama koje se nalaze na krtici. Veči deo operativnih sistema važne informacije čuva u EEPROM memoriji u šifrovanom obliku tako da je vrlo teško dobiti otvoreni tekst hakerisanjem EEPROM memorije. Drugi vid fizičkog napada koji se pokazao kao uspešan jeste intenzivna fizička fluktacija u određeno vreme i na određenom mestu gde se obavlja potvrđivanje PIN koda. Zato se mogu izvršavati i određene funkcije bez PIN koda. Ovakvi napadi se mogu kombinovati sa logičkim napadima da bi se došlo do tajnog ključa. Većina fizičkih napada zahteva posedovanje određene vrste opreme.

11.3. Trojanski konji

Ovi napadai su se pojavili na taj način što se u radnoj stanici neopreznog korisnika pojavljuju i zadržavaju određene aplikacije. Princip rada trojanskog konja jeste da sačeka da korisnik unese svoj PIN kod pri čemu omogućava upotrebu tajnog ključa što omogućava aplikaciji da pozove da se digitalno potpišu neki zlonamerni kodovi. Operacija vezana za trojanskog konja počinje i završava se, a korisnik nije svestan činjenice da je njegov tajni ključ upotrebljen mimo njegove volje. Zaštita od ovakvih napada je korišćenje arhitekture "single–access devide driver". Ovakva arhitektura jača operativni sistem tako da samo jedna aplikacija može priustupiti serijskom uređaju, pa tako i smart kartici u bilo kom trenutku. Još jedan način za sprečavanje trojanskog konja je korišćenje modela kojim se dozvoljava upotreba samo jednog tajnog ključa za svaki unos PIN koda. Kod ovog načina korisnik mora da unese svoj PIN svaki put kada se koristi tajni ključ tako da trojanski konj nema pristup ključu.

11.4. Napadi usmereni na nepažnju korisnika i administratora sistema

Ovaj vid napada se u računarskim sistemima pokazao kao najuspešniji pogotovu kada je oprema pravilno konfigurisana. Ono na šta se obraća pažnja prilikom ovih napada su greške prouzrokovane ljudskim faktorom. Primer ovakvog napada je kada se napadač predstavlja kao administrator mreže. On na taj način pristupa sistemu i zahteva lozinke korisnika za bavljanje različitih aktivnosti u mreži. Korišćenjem inteligentnih kartica se sprečava mogućnost ovakvih napada.

12.SIGURNOST SMART KARTICA

Najvažnije obeležje smart kartica predstavlja sigurnost. To je često primarna važnost pre svega kod finansijskih aplikacija i u slučaju kada se radi o privatnosti podataka. Za razliku od recimo kartica sa magnetnom trakom smart kartica kao primer aktivnog sistema je sposobna da presretne razne napade od strane neautorizovanih osoba koje imaju nameru da recimo pročitaju sigurnosne podatke koji su smešteni na kartici. Međutim, za smat kartice se ne može reći da su u potpunosti sigurne iz prostog razloga jer se svaki sistem, ukoliko postoji dovoljan broj resursa, može ugroziti. E sada, da li sistem može da se ugrozi zavisi od toga da li je visina truda utrošenog za njegovu zaštitu veća od visina truda uloženog na to da se njegova sigurnost ugrozi. Međutim, kako god, smart kartice ipak pružaju veću mogućnost zaštite od recimo kartica sa magnetnom trakom. Uglavnom svi napadi upućeni prema smart karticama se definišu kao napadi 3.stepena što znači da su potrebni milioni dolara i stotine i stotine godina računarske snage da bi se ugrozila sigurnost jedne transakcije.

12.1. Mehanizmi sigurnosti podataka

12.1.1. Integritet podataka

Ovo je mehanizam sigurnosti koji proverava određene karakteristike dokumenata i transakcija. Ovaj mehanizam osigurava da podaci prilikom prenosa nisu korumpirani ili izgubljeni. Karakteristike dokumenata i transakcije se proveravaju da bi se utvrdilo koliko su podaci tačni i pravilno autorizovani. Integritet podataka se postiže uz pomoć električne kriptografije koja dodeljuje jedinstven identitet podacima kao što je npr.otisak prsta. Na taj način promena tog identiteta signalizira neku promenu i na taj način se može saznati da li su podaci podložni promeni ili ne.

12.1.2. Autentičnost

Kod ovog mehanizma se prvo ispituje a zatim se potvrđuje pravilan identitet onih koji učestvuju u transakciji podataka. Digitalni potpis proverava podatke i njihovo poreklo i procesuira identitet koji sve strane koje učestvuju u transakciji mogu uzajamno da provere. Digitalni potpis se procesuira uz pomoć kriptografskog hash algoritma a temelji se na faktorima velikih primarnih brojeva.

12.1.3. Nerazdvojivost

Ovaj mehanizam eliminiše mogućnosti dodavanja ili razdvojivosti digitalnog potpisa u poruku, kod koje bi druga strana digitalni potpis proglasila kao tačan.

12.1.4. Autorizacija

Autorizacija je mehanizam u kojem se dozvoljava pristup posebnim podacima. Na taj način se mogu postaviti privilegije upravljanja nekim podacima od strane određenih osoba.

12.1.5. Poverljivostt / Kriptografija

Poverljivost predstavlja mehanizam koji koristi postupak kriptografije kako bi se zaštitile informacije od neautorizovanog pristupa. Kao primer tome se može uzeti običan tekst koji je pretvoren u šifrovani oblik uz pomoć nekog algoritma a zatim je odšifriran u običan tekst istim postupkom. Kriptografija je metoda pretvaranja podataka iz oblika koji je čitljiv ljudima u neki drugi oblik a zatim ponovnog pretvaranja u njegov čitljivi oblik kako bi se došlo do toga da se oteža pristup neovlašćenim osobama.

Kriptografija se koristi u sledećim slučajevima:

- U osiguravanju privatnosti podataka, kriptovanjem podataka,
- U osiguravanju integriteta podataka, prepoznavanjem da li su podaci bili podvrgnuti neovlašćenom postupku.

U osiguravanju jedinstvenosti podataka se koristi proveravanjem da li je reč o originalnoj poruci ili je reč o kopiji originala. Pošiljaoc porukle dobija neki jedinstveni identitet koji zatim primaoc poruke proverava. Originalni podaci mogu da budu u obliku koji je čitljiv ljudima (tekst fajl) ili u obliku koji prepoznaju računari (baza podataka, slika i sl.) Originalni podaci se nazivaju nekriptovanim podacima ili običnim tekstom dok se podaci koji su dobijeni kriptografskim postupkom nazivaju kriptovanim podacima ili šifrovanim tekstom. Proces pretvaranja običnog teksta u šifrovan tekst se naziva enkripcija dok se suprotan proces tj. proces pretvaranja šifrovanog teksta u običan tekst naziva dekripcijom.

Da bi podaci mogli da se pretvaraju iz jednog u drugi oblik potrebno je da postoji enkripcijski algoritam i ključ. Ako je ključ koji je korišćen za enkripciju korišćen i za dekripciju onda se taj ključ naziva simetričnim a najpoznatiji simetrični algoritam je DES (Data Encryption Standard).

DES simetrični algoritam je izmišljen 1970.godine u IBM-u i bio je proučavan od strane kriptografa više od 20 godina za čije vreme nije bilo nikakvih metoda koje bi omogućile probijanje ove kriptografije. DES algoritam ima 56-bitni ključ. Kod simetrične enkripcije podataka problem predstavlja razmena ključeva koji se koriste za enkripciju i dektripciju podataka. Kako se i za dekripciju i za enkripciju podataka koristi isti ključ pošiljaoc poruke mora poslati primaocu poruke i ključ kojim je poruka enkriptovana. Trostruki DES (Triple DES) metoda enkripcije koristi postojeći DES algoritam na poseban način kako bi došlo do poboljšanja sigurnosti. Trostruki DES algoritam može da bude izveden sa dva ili tri ključa u zavisnosti od primene. Kako algoritam obavlja enkripciju – dekripciju – enkripciju često se naziva i EDE algoritam. Algoritam kod koga su korišćeni različiti ključevi za enkripciju i dekripciju se naziva asimetrični algoritam. Asimetrična enkripcija ima par ključeva pri čemu se jedan ključ koristi za enkripciju a komplementaran ključ iz sistema se koristi za dekripciju. Na taj način svaki korisnik može da objavi jedan ključ (javni ključ) a drugi da ostavi samo sebi poznatim (tajni ključ). Kada pošiljaoc želi da pošalje poruku može da je enkriptuje javnim ključem primaoca poruke i uz tom slučaju poruku može da pročita samo primaoc poruke kome je ona namenjena. Međutim, iako se vidi da asimetrična enkripcija ima prednosti ona se retko koristi jer je algoritam puno sporiji od simetrične enkripcije. Najpoznatiji asimetrični algoritam je RSA. Kako bi imali prednosti i simetričnog i asimetričnog algoritm moderni mehanizmi koriste simetričnu enkripciju za enkriptovanje dokumenata. Enkripcija koristi slučajno generisan ključ koji se rada enkriptuje asimetričnim algoritmom i koji se šalje zajedno sa porukom. Na taj način je ključ zaštićen a dokument se može dekriptovati bržim algoritmom.

13. ULOGA SMART KARTICA ZA SIGURNOST RAČUNARSKIH MREŽA

Pošto računari i računarske mreže polako ali sigurno zauzimaju centralno mesto u našim životima dolazi do povećavanja problema u vezi bezbednosti istih. Inteligentne kartice doprinose ovoj povezanosti i drugim dodatnim sposobnostima na taj način što obezbeđuju neophodne bezbedonosne mere koje nisu ostvarljive na drugi način. Na internetu smart kartica povećava bezbednost uz pomoć autentifikacije, autorizacije, privatnosti, integriteta i nemogućnosti odbijanja. Ovo je iz razloga jer privatni ključ za potpis nikada ne napušta inteligentnu karticu tako da je vrlo teško da se sazna sadržaj ključa. U sistemima preduzeća njihova bezbednost je zasnovana na različitim tehnologijama. Smart kartice mogu da čuvaju više sertifikata i lozinki na istoj kartici. Siguran e-mail i pristup internetu, pristup mreži, šifrovani fajlovi i kontrola ulaza u zgradu su poboljšani upotrebom smart kartice. Ukoliko bi u nekom ekstranet sistemu jedna kompanija želela da nadgleda bezbednost poslovnih partnera i dobavljača onda bi moglo da dođe do distribuiranja smart kartica i dozvole za pristup pojedinim resursima te kompanije. Koliko su inteligentne kartice važne u ovoj situaciji je vidno zbog toga što postoji potreba za najvećom mogućom bezbednošću u situaciji kada nekome dozvoljavate prolaz korz *firewall* ili *proxy*.

Neki od razloga zašto inteligentne kartice povećavaju bezbednost sistema:

PKI (*Public Key Infrastructure*) su sistemi koji su bezbedniji od sistema baziranih na lozinkama iz razloga jer nema deljenja tajnog sadržaja. Privatni ključ se mora poznavati samo na jednom mestu a ako je to mesto inteligentna kartica onda privatni ključ nikada ne napušta karticu a tajni sadržaj datog sistema se nikada ne nalazi u situaciji da ga je moguće ugorziti.

Smart kartice povećavaju bezbednost sistema zasnovanih na lozinki – i pored toga što intelignetne kartice imaju očigledne prednosti za PKI sisteme one takođe povećavaju bezbednost sistema sa lozinkama. Jedan od najvećih problema tipičnih sistema sa lozinkama je taj što korisnici svoje lozinke zapisuju i ostavljaju na mesto vidno drugim osobama. Pored toga, ljudi takođe biraju veoma slabe lozinke koje uz to i dele sa drugim ljudima. Međutim, ukoliko se kartica koristi kako bi sačuvala više korisničkih lozinki onda korisnici trebaju jedino da zapamte PIN na kartici i preko pina mogu pristupiti svim lozinkama. Krajnji korisnik nikada ne treba da zna lozinku već samo PIN tako da nema potrebe da lozinke zapisuje i deli sa drugima.

Dva faktora autentifikacije – Sigurnosni sistemi koriste više faktora za autentifikaciju. Faktori koji se obično koriste su: nešto znate, nešto imate, nešto jeste i nešto radite. Sistemi sa lozinkama koriste samo prvi faktor. Smart kartice koriste pored prvog i drugi faktor (nešto znate + nešto imate). Smart kartice pored PIN koda koriste i neke biometrijske tehnologije kao što su otisak prsta, oblik mrežnjače ili neke druge biometrijske informacije koje se mogu sačuvati na kartici samo da bi se uporedili sa podacima dobijenim od posebnog biometrijskog ulaznog uređaja. Na kartici se takođe mogu sačuvati i osobine rukom pisanog teksta ili glasa.

Prenošenje ključeva i sertifikata – Javni i tajni ključ koriste web pretraživači i drugi popularni softverski paketi, ali oni na neki način radije identifikuju radnu stanicu nego korisnika. Podaci o ključu i sertifikatu se čuvaju u odgovarajućim područjima i moraju biti eksportovani/importovani da bi se preneli od jedne do druge radne stanice. Upotrebom inteligentnih kartica se privatni ključ i sertifikat mogu prenositi i mogu biti korišćeni na više radnih stanica, bez obzira da li su one na poslu, kod kuće ili na putu. Što je nivo softverskog

sloja koji to podržava niži to se one mogu koristiti sa više različitih softverskih programa od različitih proizvođača na različitim platformama poput UNIX, Mac i Windows.

Automatsko onemogućenje PIN-a – Ukoliko bi uzeli primer čuvanja nekih podataka na hard disku koji su zaštićeni lozinkom onda bi se probijanje te lozinke moglo izvršiti višestrukim pokušajima unošenja raznih kombinacija šifri. Međutim, to je kod smart kartica onemogućeno na taj način što se posle određenog broja pogrešno unetih PINova kartica zaključava.

Nemogućnost odbijanja (*Non-Repudiation*) – Sposobnost osporavanja nakon digitalnog potpisivanja od strane ključa naziva se odricanje (*repudiation*). Ako privatni ključ postoji samo na jednoj smart kartici čiji PIN zna samo njen vlasnik jako je teško da drugi zamene digitalni potpis korišćenjem privatnog ključa vlasnika. Privatni ključ je obično zaštićen hardverski i ne može biti korišćen bez poznavanja odgovarajućeg PIN-a.

Upotreba privatnog ključa – U životu se veliki broj autorizacija vrši ručnim potpisom. Digitalni potpisi bazirani na smart kartici omogućavaju veću korist od onih koji su napisani rukom iz razloga jer je mnogo teže falsifikovati te potpise a i zbog toga što oni mogu da ojačaju integritet dokumenta različitim tehnologijama kao što je npr. haširanje. Takođe, smart kartica može da evidentira broj koliko je puta privatni ključ korišćen pri čemu daje precizan iznos korišćenja digitalnog potpisa u odnosu na dati vremenski period.

14.PROIZVODI I APLIKACIJE KOJE KORISTE SMART KARTICE

Smart kartice se često koriste u sledećim aplikacijama:

WEB pretraživači (*WEB browsers*)

WEB pretraživači dok čitaju sadržaje sa *World WIDE Web*-a koriste različite tehnologije za sigurnost poput SSL (*Secure Sockets Layer*) i TLS (*Transport Layer Security*). Ove tehnologije mogu da izvršavaju autentifikaciju klijenta iili servera prema drugom klijentu i/ili serveru i takođe obezbeđuju kriptovan kanal za bilo kakav saobraćaj (poruka ili prenos datoteka). Autontičnost je ojačana iz razloga jer se privatni ključ nalazi na kartici. Kriptovani kanal obično koristi simetrično šifrovanje pri čemu se šifrovanje izvršava na host računaru iz razloga male brzine prenosa podataka od i ka inteligentnoj kartici. Slučajno generisan ključ, koji se koristi za simetrično šifrovanje je upakovan zajedno sa javnim ključem partnera u komunikaciji što znači da on može da se raspakuje samo na inteligentnoj kartici. Zbog toga je veoma teško za onoga ko prisluškuje komunikaciju da dobije ikakvo saznanje o ključu korišćenom u ovoj sesiji kao i o poruci koja se prenosi.

Siguran Email (*S/MIME, OpenPGP*)

Tehnologije koje dozvoljavaju da se mejl poruke šifruju i/ili digitalno potpisuju su S/MIME i OpenPGP. Kao i kod SSL-a inteligentne kartice jačaju sigurnost ovih operacija na taj način što štite tajnost privatnog ključa a i pored toga raspakuju ključeve u sigurnom okruženju.

Potpisivanje formulara (*Form Signing*)

HTML formulari koji su bazirani na WEB-u mogu da se digitalno potpisuju samo uz pomoć privatnog ključa. iz razloga jer omogućava da digitalni dokumenti budu hostovani na WEB serveru i da može da im se pristupi pomoću WEB pretraživača u elektronskoj formi ovaj način se pokazao kao vrlo važna tehnologija. Smart kartice koje služe za potpisivanje formulara omogućavaju prenos privatnog ključa kao i hardversku nemogućnost odbijanja poruke.

Potpisivanje objekata (*Object Signing*)

Ako neka organizacija napiše kod koji može biti downloadovan sa WEB – a a zatim da se izvrši na nekom klijentskom računaru najbolje je da se taj kod potpiše tako da klijent može da bude siguran da je kod zaista došao iz željenog izvora. Smart kartica može da se upotrebi u organizaciji koja potpisuje poruku tako da privatni ključ ne može da bude ugrožen od napadača koji se izdaje za pravog potpisnika.

Prednosti *kiosk/portable* moda

Neke aplikacije najbolje rade u portabl modu gde se jedan računar koristi od strane više korisnika ali se on prekonfiguriše za odgovarajućeg korisnika kada on ubaci svoju inteligentnu karticu u određeni čitač. Računar se može koristiti za siguran mejl, čitanje web sadržaja i sl. Privatni ključ nikada ne napušta inteligentnu karticu. Taj ralunar se može konfigurisati na taj način da ne prihvata nikakve naredbe sa odgovarajućeg ulaznog uređaja sve dok korisnik je ubaci odgovarajuću karticu i odgovarajući PIN kod.

Šifrovanje datoteka (*File Encryption*)

Iako smart kartice sa brzinom protoka od 9600 bound-a obično ne predstavljaju pogodan mehanizam za formiranje velikih šifrovanih datoteka one ipak pojačavavaju sigurnost ove funkcije. U drugom slučaju, slučajno generisan ključ se koristi za svaku datoteku koja se šifruje; formiranje velikih šifrata se može izvršiti na host računarskom sistemu sa većim brzinama i ključ u sesiji se tek onda može upakovati u karticu. Tada je jedini način da se lako dešifruje datoteka tak da se poseduje ispravna kartica i da se unese pravilan PIN kod tako da ključ može da se raspakuje.

Sigurnost elektronskih transakcija (*Secure Electronic Transaction*-SET)

SET protokoli omogućavaju da se podaci sa kreditnih kartica bezbedno prenose između korisnika, trgovaca i izdavača. Pošto se SET oslanja na tehnologije javnog ključa, inteligentne kartice su dobar izbor za čuvanje sertifikata i javnog ključa.

Digital Cash (novac u elektronskoj formi)

Inteligentne kartice sadrže protokole pomoću kojih se može čuvati novac na inteligentnoj kartici. U ovakvim sistemima osnovni ključ koji obezbeđuje arhitekturu nikada ne napušta bezbedno područje hardverskog uređaja. *Mondex*, *VisaCash*, *EMV* i *Proton* su primeri ovih protokola dizajniranih za upotrebu u inteligentnim karticama.

15. PREDNOSTI SMART KARTICA

U odnosu na recimo kartice sa magnetnom trakom Smart kartice nude poboljšanu sigurnost, prikladnost i ekonomske pogodnosti. Pored toga Smart kartice imaju visok stepen podešavanja u skladu sa individualnim potrebama.

15.1. Sigurnost

Smart kartice koriste spoj enkripcije koje mogu obavljati izdavačke i korisničke zahteve sa najvećim stepenom sigurnosti. Koristeći enkripciju podaci mogu da se sigurno prenesu preko običnih ili "wireless" mreža. U kombinjaciji sa biometričkim metodama identifikacije (npr. otisak prsta) Smart kartice se koriste za distribuciju državnih sredstava tamo gde je to potrebno, reducirajući tako mogućnost zloupotrebe i prevare. Smart kartice zdravstvenog osiguranja omogućuju doktorima i osoblju pristup pacijentovoj povijesti bolesti, bez ugrožavanja privatnosti.

15.2. Prikladnost

Jedna od prednosti smart kartica je ta što će zameniti različite identifikacione kartice. Smart kartice će biti kombinacija papirne, plastične i magnetske kartice koje su bile korištene za identifikaciju, kartice koje dozvoljavaju kopiranje, naplatu telefonskih razgovora u telefonskim govornicama, penzijske i zdravstvene podatke. Zdravstvo će npr. da smanji troškove obrade baze podataka svih pacijenata, tako da če omogućiti pristup ličnim podacima pacijenta koji se nalaze direktno na Smart kartici.

15.3. Ekonomske pogodnosti

Smart kartice smanjuju troškove transakcija tako što eliminišu papir i troškove obrade podataka na papiru u bolnicama i državnim službama. Kontaktne i bezkontaktne smart kartice bi mogle recimo da omoguće modernizaciju recimo sistema za naplatu putarine, tako što će smanjiti troškove radne snage kao i kašnjenja koja uzrokuju postojeći sistemi. Naplate na benzinskim pumpama, naplate parkiranja i naplate telefonskih razgovora se uz pomoć smart kartica mogu smanjiti dok prihodi mogu čak i da se povećajuzbog njihove primene.

15.4. Svestranost

Smart kartice sadrže sve podatke potrebne za lični pristup mreži, pristup internetu, plaćanje i druge aplikacije. Koristeći Smart karticu moguće je uspostaviti direkntu vezu sa mrežom bilo gde u svetu koristeći se telefonom. Web serveri će proveriti korisnički identitet i predstaviti web stranicu, e-mail ili bilo koji drugi web servis na osnovu podataka pročitanih sa kartice. Lična podešavanja potrebna za elektronsku primenu će biti radije smešteni na karticu nego u aplikacijama. Dok se aplikacije menjaju, korisnik nosi sve na kartici koristeći je kao osnovni mrežni i računarski uređaj.

16. ZAKLJUČAK

U ovom pristupnom radu je opisana struktura smart kartice kao i glavni način njene primene i zaštite. U ovom radu smo videli kako smart kartica svojim razvojem utiče na ubrzani razvoj sistema za autentifikaciju korisnika.

Upotreba kartica u današnje vreme postaje sve veća a upotreba smart kartica i zamena za dosadašnje kartice sa magnetnom trakom postaje sve učestalija. Danas upotreba kartica u svakodnevnom životu postaje sve veća. Mogućnosti kartica se povećavaju iz dana u dan tako da vremenom jedna kartica dobija na univerzalnosti tj.javlja se sve više mogućnosti koje jedna kartica može da obavi. Kao primer se mogu uzeti zemlje Zapadne Evrope koje su napravile sistem za korišćenje smart kartica u zdravstvu i na taj način sve kartone i zdravstvenu evidenciju pacijenata smestile na jednu karticu.

Sa daljim razvojem smart kartica može se očekivati da će u budućnosti jedna smart kartica obavljati ulogu vozačke dozvole, lične karte, zdravstvene knjižice, raznih članskih karti, da će obavljati ulogu kartica za mobilne telefone i bankomate, kartica za pristup sigurnosnim mrežnim sistemima i sl. Ukoliko se u obzir uzme dalji razvoj smart kartica i pre svega karakteristike super smart kartica koje sam naveo u poglavlju 5 onda se može doći do zaključka da će upotreba kartica i pre svega njihova mobilnost umnogome olakšati i ubrzati život ljudi.

Na kraju bi trebalo samo, što se sigurnosnog dela tiče, istaći da je smart kartica (ukoliko se prilikom njene proizvodnje poštuju neki standardi kao i prilikom korišćenja poštuju neka pravila) izuzetno siguran uređaj. Kao takav uređaj ona predstavlja sigurno mesto za čuvanje vrednih podataka kao što su privatni ključevi, brojevi računa u bankama, biometrijske informacije i sl. Pored toga ona predstavlja i sigurno mesto na kojem se u offline obliku mogu obavljati procesi kao što je enkripcija i dekripcija privatnog ili javnog ključa. Na osnovu svega napred iznetog u vezi sigurnosti smart kartica može se zaključiti da smart kartica može da postane odlično rešenje za sigurnosne probleme u svetu.

17. Literatura

- W. Rankl – W. Effing: *Smart Card Handbook,* John Wiley & Sons, 1997.
- J. L. Zoreda – J. M. Oton: *Smart Cards*, Artech House, 1994.
- http://en.wikipedia.org/wiki/ISO/IEC_7810
  (Posećeno: 26.06.2009.godine)
- http://en.wikipedia.org/wiki/ISO/IEC_7813
  (Posećeno: 26.06.2009.godine)
- http://en.wikipedia.org/wiki/ISO/IEC_7810
  (Posećeno: 26.06.2009.godine)
- http://en.wikipedia.org/wiki/ISO/IEC_7811
  (Posećeno: 26.06.2009.godine)
- www.tech-faq.com
  (Posećeno: 27.06.2009.godine)
- http://www.tech-faq.com/ISO-7816.shtml
  (Posećeno: 27.06.2009.godine)