3. INTELIGENTNE KARTICE (Smart Card)

3.1. Istorija inteligentnih kartica

Korijeni današnjih inteligentnih kartica potiču iz ranih 50-ih kada je Diners Club u SAD proizveo prvu potpuno plastičnu karticu koja se koristila kao sredstvo plaćanja. Korišten je sintetički PVC materijal tako da je nastala izdržljivija kartica (dugotrajnija) za razliku od prethodne kartice bazirane na papiru. U ovom sistemu kartica vas je, ustvari, identifikovala kao člana izabrane grupe i bila je prihvaćena od strane izvjesnih restorana i hotela koji su respektovali pripadnike ove grupe. VISA i MasterCard su se tada pojavili na tržištu, ali zbog neovlaštenog miješanja potreba trgovaca i banaka neophodno je bilo da se napravi kartica koja bi se očitavala pomoću određenog uređaja. Pojavila se magnetna traka koja je omogućila dalju digitalizaciju podataka koji su bili sačuvani na kartici u formatu pogodnom za očitavanje putem nekog uređaja. Ovaj tip kartica sa magnetnom trakom je donedavno bio najčešće korišten metod plaćanja. Tehnologija magnetnih traka posjeduje određene slabosti zbog kojih bilo ko sa pristupom odgovarajućem uređaju može čitati, upisivati ili brisati podatke. Stoga kartica sa magnetnom trakom je nepogodna za čuvanje osjetljivih podataka i kao takva zahtijeva centralnu, *on-line*, pozadinsku infrastrukturu za verifikaciju i obradu. Pošto se pojavila, ova kartica sa pozadinskom infrastrukturom je bila raspoloživa u SAD, ali ne i u evropskim zemljama. Kao u bilo kojoj klijent/server arhitekturi jedno rješenje je trebalo da bude ojačanje pozadinske strane (strane servera), a drugo rješenje je da osnaži klijentsku stranu prebacujući dio aktivnosti sa servera na klijenta. Čini se da su evropske zemlje radije koristile pristup vezan za stranu klijenta i napravile su ogromna poboljšanja uvodeći u upotrebu kartice sa integrisanim kolom (*Integrated Circuit Card*-ICC). Godine 1968. njemački naučnici Juergen Dethloff i Helmut Groetrupp su prijavili prvi patent povezan sa karticama sa integrisanim kolom. Slične aplikacije su uslijedile u Japanu 1970. i Francuskoj 1974. godine. 1984. godine francuski PTT je uspješno izvršio probnu upotrebu telefonskih kartica. Do 1986. godine više miliona francuskih telefona sa inteligentnim karticama je bilo u upotrebi. Njihov broj je dostigao blizu 60 miliona u 1990. godini i 150 miliona u 1996. godini. Nakon što je kriptografija učinila napredak u 60-im i pošto su se bezbjednosni mehanizmi mogli dokazati matematički, inteligentne kartice su se dokazale kao idealan medijum za sigurno čuvanje kriptografskih ključeva i algoritama. Francuske banke su bile prvo područje djelovanja ovih kartica u 1984. godini. Njemačke banke su počele sa uvođenjem u upotrebu 1997. godine. Druga primjena inteligentnih kartica u Njemačkoj uključuje 70 miliona ovih kartica koje u sebi sadrže informacije o zdravstvenom osiguranju korisnika.

3.2. Tipovi kartica

Međunarodna organizacija za standardizaciju (ISO) svojim standardom 7810: ″Identifikaciona kartica - fizičke karakteristike″ definiše fizičke osobine kao što su fleksibilnost, temperaturni opseg i dimenzije za tri različita formata kartica (ID-1, ID-2 i ID-3). Standard za inteligentne kartice, ISO 7816 je zasnovan na ID-1 formatu. U ovom poglavlju se opisuje nekoliko različitih vrsta ID -1 kartica. Jedan tip kartica je posebno značajan, tzv. kriptografska koprocesorska kartica, koja postaje vrlo važna za bezbjednost računarskih mreža i PC sistema.

***Embossed* (Kartica sa ispupčenjima)**

Ispupčenja omogućavaju da tekstualne informacije sa kartice budu prebačene na papir korištenjem jednostavnih i jeftinih uređaja. ISO 7811 specificira formu, veličinu, visinu ispupčenja, kao i poziciju. Prenos informacija preko ispupčenja može se činiti primitivnim, ali jednostavnost ovog sistema ga je učinila široko rasprostranjenim.

Magnetna traka

Osnovna prednost koju nudi tehnologija magnetnih traka, u odnosu na kartice sa ispupčenjima je smanjenje obilne papirne dokumentacije. Poglavlja 2, 4 i 5 standarda ISO 7811 specificiraju karakteristike magnetne trake, tehnike kodovanja i pozicije. Kapacitet memorije za čuvanje podataka

magnetnih traka je oko 1000 bita i bilo ko sa upisno/čitajućim uređajem može vidjeti i/ili izmijeniti podatke.

Inteligentne kartice

Inteligentnim karticama se obično smatraju kartice sa integralnim kolom. One su najnoviji i najpametniji dio u porodici ID-1 i zasnovane su na seriji standarda ISO 7816. Ovi tipovi kartica pružaju daleko veće mogućnosti i kapacitete čuvanja podataka. Vjerovatno najvažnije je da podaci koji se čuvaju mogu biti zaštićeni protiv neovlaštenog pristupa, miješanja i ugrožavanja. Funkcije vezane za memoriju kao što su čitanje, upisivanje i brisanje mogu biti vezane za specifične uslove, upravljane i od hardvera i od softvera. Druga prednost inteligentnih kartica je i njihova veća pouzdanost i duži vijek trajanja.

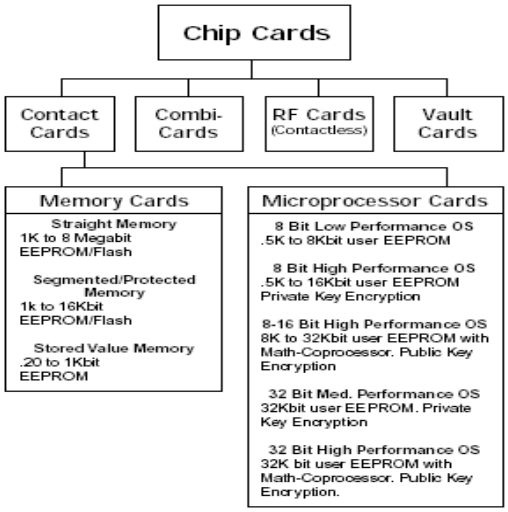
Inteligentna kartica je plastična kartica sa ugrađenim čipom koja skladišti i prenosi podatke između korisnika. Ovi podaci imaju veze ili sa vrijednošću, korisnom informacijom i skladište se i obrađuju unutar čipa na kartici ili se čuvaju u memoriji. Podaci na kartici se prenose preko čitača koji je dio računarskog sistema. Osnaženi sistemi inteligentnih kartica su danas u širokoj upotrebi zahvaljujući nekolicini ključnih aplikacija uključujući zdravstvenu zaštitu, bankarstvo, preduzetništvo i transport. Sve aplikacije mogu imati koristi od dodatnih pogodnosti i bezbjednosti koje omogućava inteligentna kartica. Prema najnovijim istraživanjima tržište inteligentnih kartica će narasti do 6,8 milijardi jedinica u 2002.godini.

Memorijske kartice (*Memory Cards*)

Iako vezane za inteligentne kartice, memorijske kartice su manje funkcionalne i mnogo jeftinije od mikroprocesorskih kartica. One u sebi imaju EEPROM i ROM memoriju, kao i određenu adresu i logiku vezanu za bezbjednost. U najjednostavnijem obliku logika postoji da spriječi upisivanje i brisanje podataka. Kompleksniji dizajn dozvoljava da se ograniči mogućnost čitanja memorije. Tipične aplikacije memorijske kartice su pre-paid telefonske kartice i kartice za zdravstveno osiguranje (*health insurance card*).

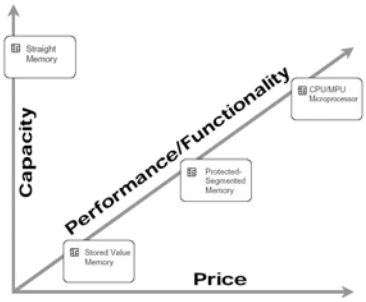
3.3. Tipovi čip kartica

Inteligentne kartice predstavljaju tehnologiju koja omogućava različite primjene lako prilagodljive potrebama korisnika. Stoga poznavanje prirode inteligentne kartice omogućava stvaranje razumljivog koncepta i efikasnih sistema.



Slika 1 - tipovi čip kartica

Inteligentna kartica je veličine kreditne kartice. Ima ugrađen poseban tip integralnog kola koji čuva informacije u elektronskoj formi i upravlja upotrebom i načinom korištenja ovih podataka. Ovim podacima se može lako, bezbjedno i precizno pristupiti pomoću različite opreme za obradu podataka u elektronskoj formi. Ova jedinstvena kombinacija znači da je inteligentna kartica medij za prenos informacija i interfejs između korisnika i mašine.



Inteligentne kartice se definišu u skladu sa vrstom čipa ugrađenog u karticu i njegovih sposobnosti. Postoji veoma mnogo mogućnosti koje se mogu izabrati kada dizajniramo neki sistem.

Povećani nivo mogućnosti obrade, fleksibilnost i količina memorije povećavaju troškove. Kartice sa jednom funkcijom su često najefikasnije rješenje. Treba se izabrati pravi tip inteligentne kartice za odgovarajuću aplikaciju upoređujući troškove,

funkcionalnost i zahtijevani nivo bezbjednosti. Prethodna slika demonstrira opšta pravila.

3.3.1. Memorijske kartice

Memorijske kartice ne mogu dinamički upravljati datotekama. Sve memorije komuniciraju sa čitačima preko sinhronih protokola. Postoje tri osnovna tipa memorijskih kartica:

Čisto (Straight) memorijska kartica

Ove kartice samo čuvaju podatke i nemaju sposobnost njihove obrade. Ove kartice imaju najmanje troškove po bitu za korisničku memoriju. One se smatraju kao flopi disk različitog kapaciteta bez mehanizma za zaključavanje. Ove kartice ne mogu se identifikovati prema čitaču tako da host sistem mora znati koji tip kartice je ubačen u čitač.

Zaštićene/segmentirane memorijske kartice

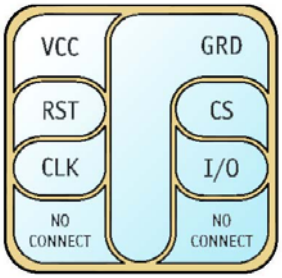
Ove kartice imaju ugrađenu logiku za kontrolu pristupa do memorije na kartici. One mogu biti konfigurisane tako da ograničavaju mogućnost i čitanja i upisivanja na karticu. Ovo se obično radi koristeći lozinku ili sistemske ključeve. Segmentirane memorijske kartice mogu biti podijeljene na logičke sekcije u slučaju planirane višefunkcionalnosti (*Multi-functionality*).

Memorijske kartice za čuvanje vrijednosti

Ove kartice su dizajnirane u svrhu čuvanja vrijednosti ili tokena. Kartice se ili izbacuju poslije upotrebe ili ponovo upisuju. Najčešće se za kartice ovog tipa preduzimaju mjere zaštite u procesu proizvodnje uključivanjem lozinki i logike koji su kodovani u čipu od strane proizvođača. Raspored memorije je setovan kao opadajući niz ili brojač. Ostaje vrlo malo memorije za ostale funkcije. Za jednostavnu primjenu kao što je telefonska kartica, čip ima 60 ili 12 memorijskih ćelija, jednu za svaku telefonsku jedinicu. Memorijska ćelija se briše svaki put kada se telefonska jedinica koristi. Jednom kada su sve memorijske jedinice iskorištene kartica postaje beskorisna i može se baciti. Ovaj proces može biti ponovljen u slučaju kartica koje se mogu puniti (Rechargeable Cards).

3.3.2. CPU / MPU mikroprocesorske višefunkcionalne kartice

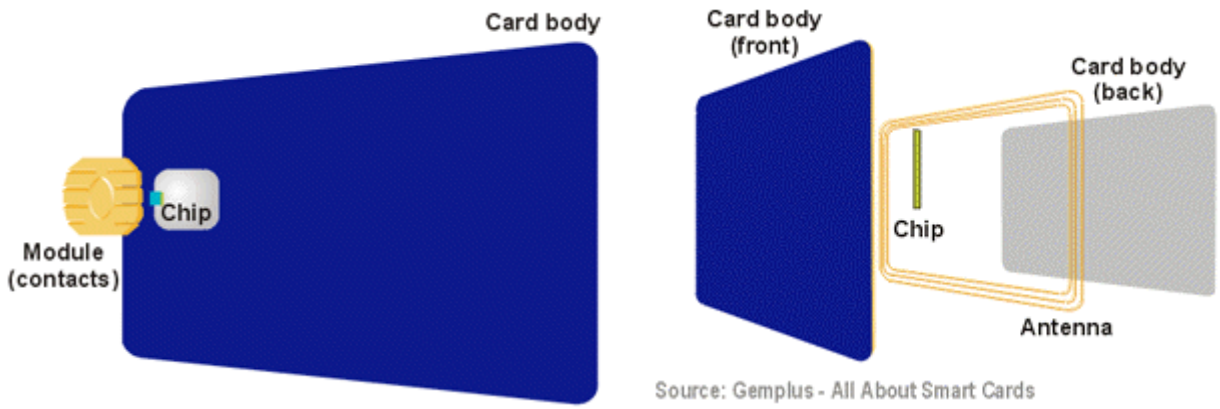
Ove kartice imaju sposobnost dinamičke obrade podataka na samoj kartici. Višefunkcionalne inteligentne kartice dijele memoriju na kartici na nezavisne sekcije dodijeljene specifičnim funkcijama ili aplikacijama. Unutar kartice je mikroprocesorski ili mikrokontrolerski čip koji upravlja dodjeljivanjem memorijske lokacije i pristupom datotekama. Ovaj tip čipova je sličan onima koji se mogu naći unutar svih personalnih računara i kada se ugrade u inteligentne kartice upravljaju podacima u organizovanim strukturama datoteka preko operativnog sistema namijenjenog inteligentnim karticama. Za razliku od drugih operativnih sistema ovaj softver kontroliše pristup korisničkoj memoriji na kartici. Ova sposobnost dozvoljava različite i multiplicirane funkcije i/ili da se različite aplikacije nalaze na kartici. Proizvođači se fokusiraju na rješenja softvera i hardvera tako da provode višeprimjenjive sisteme kartica sa manjim stepenom rizika, npr. CardLogix nudi moćne 8 i 16-bitne CMOS mikrokontrolere koji imaju svoj operativni sistem u čipu. Set komandi ovog operativnog sistema je dodatno ojačan korištenjem aplikativnog programskog interfejsa (API).



Slika 2 - Kontakti na ~ipu

Procesor na inteligentnoj kartici	PC CPU
8-bitne mašine	32-bitne mašine
brzine 3.57 MHz	do brzine 1 GHz i više

Tabela 1- poređenje mikroprocesora na kartici i PC CPU



Slika 3 - Kontaktna i beskontaktna inteligentna kartica

Mikroprocesorske kartice

Arhitektura ovog tipa kartica uključuje slijedeće komponente: CPU, RAM, ROM i EEPROM. Operativni sistem se obično nalazi u ROM-u, centralna procesorska jedinica (CPU) koristi RAM kao svoju radnu memoriju i većina podataka se čuva u EEPROM-u. Pravilo koje se poštuje je da RAM zahtijeva četiri puta veći prostor od EEPROM-a, koji opet traži četiri puta veći prostor od ROM-a. Karakteristike konvencionalnih arhitektura inteligentnih kartica su date u slijedećoj tabeli:

RAM	256 bajta do 1 kilobajt
EEPROM	1 kilobajt do 16 kilobajta
ROM	6 kilobajta do 24 kilobajta
mikroprocesor	8 bita na približno 5MHz
brzina interfeja	9600 bps minimalno, poludupleksni prenos

Tabela 2- karakteristike arhitektura inteligentnih kartica

Kriptografska koprocesorska kartica

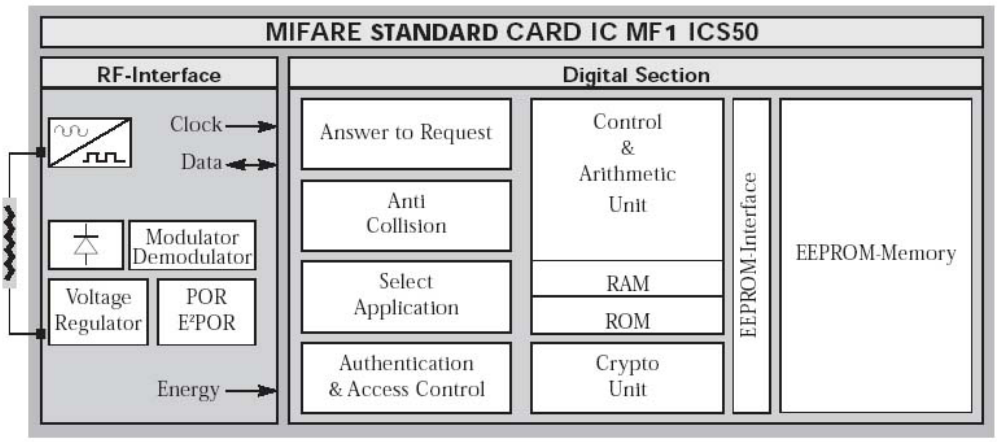
Pošto uobičajeni asimetrični kriptografski algoritmi (npr. RSA) zahtijevaju veliki broj matematičkih proračuna, jednom osmobitnom mikroprocesoru sa veoma malo RAM memorije je potrebno nekoliko minuta da obavi 1024 -bitnu operaciju vezanu za privatni ključ. U svakom slučaju, ukoliko se kriptografski mikroprocesor doda standardnoj arhitekturi, vrijeme potrebno za istu operaciju iznosi nekoliko stotina mikrosekundi. Koprocesor uključuje dodatne aritmetičke jedinice posebno razvijene za određene aritmetičke i eksponencijalne operacije. Dakako, postoji i mana ovakvih rješenja sa koprocesorima, a to je cijena koja može da se poveća od 50-100%. Uprkos povećanju troškova, ovakvo rješenje je često u upotrebi, jer je bezbjednost računarskih mreža značajno uvećana korištenjem kriptografskih koprocesora zbog toga što oni omogućavaju da privatni ključ nikada ne napušta karticu. Kao što se može vidjeti, ovo postaje kritični faktor za operacije kao što su digitalni potpis (*digital signature*), autentičnost i nemogućnost odbijanja (*non-repudiation*) poruke ili naredbe. Mada, uskoro će prestati potreba za dodatnim kriptografskim koprocesorima, jer će osnovni procesori postati dovoljno moćni da izvršavaju intenzivne matematičke operacije ili će drugi algoritmi, kao što su oni zasnovani na tehnologiji eliptičnih krivih (*elliptic curve*), postati popularni.

Beskontaktne inteligentne kartice

Iako je pouzdanost kontakata na inteligentnim karticama poboljšanja do vrlo prihvatljivog nivoa tokom niza godina, kontakti su i dalje jedan od najčšešćih problema koji se javljaju u elektromehaničkom sistemu kao posljedica prašine, prljavštine, habanja, itd.

Beskontaktna kartica rješava ovaj problem i takođe omogućuje korisniku širok opseg novih mogućnosti prilikom korištenja. Nema više potrebe da se kartice ubacuju u čitač. Kontakti na čipu nisu više vidljivi na površini kartice. Uprkos ovim beneficijama, beskontakne kartice još uvijek nisu šire prihvaćene. Veći su troškovi i čini se da proizvođači još nemaju dovoljno iskustva da bi učinili ovu

tehnologiju pouzdanom. Pretpostavlja se da će ovo elegantno rješenje vjerovatno uskoro u potpunosti zaživjeti.



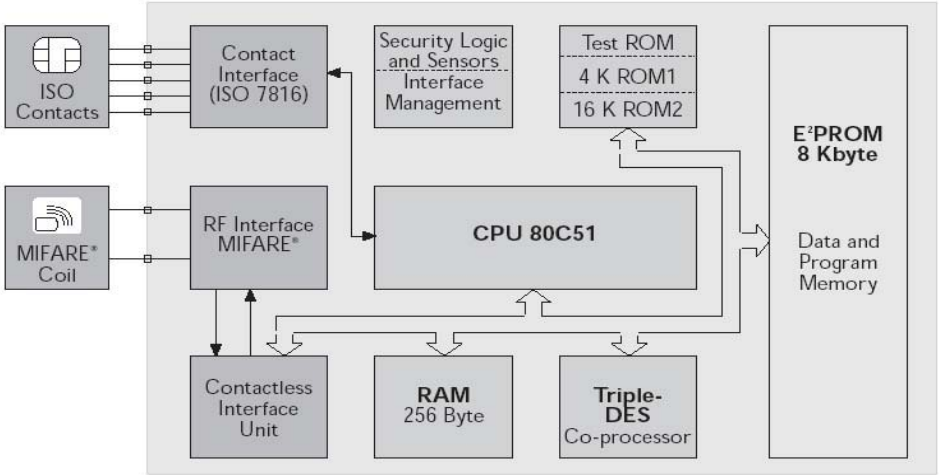
Slika 4 - Struktura jedne beskontaktne inteligentne kartice

Optičke memorijske kartice

ISO/IEC standardi 11693 i 11694 definišu standarde za optičke memorijske kartice. Ove kartice mogu nositi više megabajta podataka, ali ove kartice se mogu upisati samo jednom bez mogućnosti brisanja sa današnjom tehnologijom. Stoga su uređaji za čitanje i upisivanje za optičke kartice vrlo skupi i mogu naći svoju primjenu u zdravstvenoj zaštiti gdje se mora čuvati ogroman iznos podataka.

Hibridne (kombinovane) kartice

Najbolje rješenje, u odnosu na predhodno pomenute osobine kontaktnih i beskontaktnih kartica predstavlja kombinovana inteligentna kartica.



Slika 5- Struktura MIFARE kombinovane kartice

3.4. Primjena

Mnoge grane industrije su iskoristile moć inteligentnih kartica i ugradili ih u svoje proizvode kao što su GSM Mobilna telefonija ili TV satelitski dekoderi. Inteligentne kartice uveliko poboljšavaju bezbjednost bilo kakve transakcije. One obezbjeđuju potpuno sigurno čuvanje identiteta korisnika i njegovog računa. Inteligentne kartice također obezbjeđuju vitalne komponente za bezbjednost sistema za

razmjenu podataka kroz virtualne mreže bilo kog tipa. One štite podatke od širokog spektra prijetnji sigurnosti, od nepažljive upotrebe i čuvanja korisničkih lozinki do sofisticiranih udara na sistem. Višefunkcionalne kartice takođe mogu služiti za pristup mrežnom sistemu i skladištenje podataka. Ljudi širom svijeta danas koriste inteligentne kartice za različite dnevne poslove i zadatke koji uključuju:

Lojalnost i čuvanje podataka

Za višelančanu trgovinu koja vodi računa o programima u više različitih poslova inteligentne kartice mogu iz jednog centra locirati i pratiti sve podatke. Primjene su brojne od parkiranja i odlazaka u perionice veša, pa sve do bilo kakve upotrebe u trgovini i preduzeću.

Bezbjednost informacija i fizičkih sredstava

Kao dopuna bezbjednosti informacija, inteligentne kartice postižu veću fizičku bezbjednost servisa i opreme, zbog toga što kartica ograničava pristup svim, izuzev ovlaštenim korisnicima. E-mail i personalni računari se zaključavaju inteligentnom karticom. TV sistemi prihvataju inteligentne kartice kao elektronski ključ za zaštitu. One takođe djeluju kao ključevi za pristup osjetljivim laboratorijama, dispanzerima za drogu, zdravstvenu zaštitu, itd.

Elektronska trgovina (*E-Commerce*)

Inteligentne kartice olakšavaju korisnicima sigurno čuvanje informacije i gotovine za kupovinu. Prednosti koje se nude korisnicima su:

- kartica sadrži lični račun, kredit i informacije o kupovnoj moći korisnika kojima se može pristupati sa klikom miša umjesto ispunjavanja različitih obrazaca
- kartice mogu upravljati i kontrolisati troškovima sa automatskim ograničenjima i izvještavanjem
- mikroplaćanje-plaćanje nominalnih troškova bez uzimanja provizije povezano sa kreditnim karticama ili za iznose koji su previše mali za plaćanje gotovinom

Finansijsko poslovanje

Pošto banke uvode takmičenje na novootvorenim tržištima kao što su investicioni poslovi, one povećavaju bezbjednost prenosa koristeći inteligentne kartice. To znači:

- ovo će poboljšati uslugu korisnika, koji mogu koristiti bezbjedne inteligentne kartice za brze, 24 sata dostupne elektronske transfere novca preko Interneta,
- troškovi su smanjeni, transakcijama koje bi obično zahtijevale vrijeme zaposlenih u banci i ispunjavanje određenih obrazaca, može se upravljati elektronskim putem od strane korisnika sa odgovarajućom inteligentnom karticom.

Zdravstvena zaštita (*Health Care*)

Eksplozija podataka u zdravstvenoj zaštiti donosi nove izazove u efikasnijoj zaštiti pacijenata i njihove privatnosti. Inteligentne kartice rješavaju ovaj izazov sigurnim čuvanjem i distribucijom svega, od podataka u hitnim slučajevima do pogodnosti koje im se pružaju.

- brza i laka identifikacija pacijenata - poboljšani tretman,
- pogodan način da nosi podatke između sistema ili do sajtova bez sistema,
- smanjenje troškova održavanja dokumentacije.

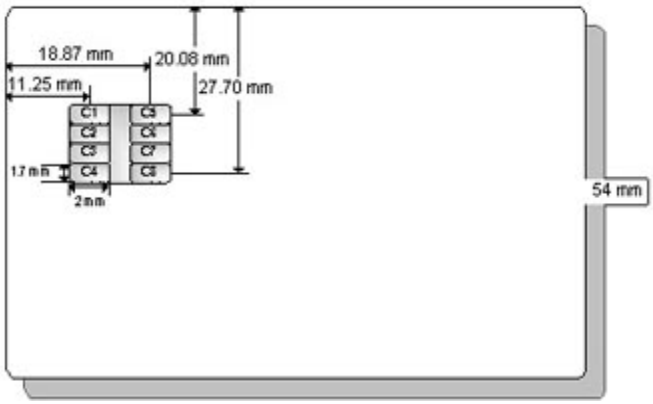
Bezbjednost telekomunikacionih i korporacijskih mreža

Intranet i virtuelne privatne mreže (*Virtual Private Networks* - VPNs) su ojačane upotrebom inteligentnih kartica. Korisnici mogu biti autentifikovani i ovlašteni da imaju pristup do specifičnih informacija zasnovanih na prethodno dodijeljenim pravima.

Pristup i kontrola ulaza

Kompanije i univerziteti bilo kog tipa trebaju jednostavne identifikacione kartice za sve zaposlene i studente. Većini njih je dozvoljen pristup do izvjesnih podataka, opreme i odjeljenja u skladu sa njihovim statusom. Višefunkcionalne, mikroprocesorske inteligentne kartice povezuju identitet sa pravima pristupa korisnika i takođe čuvaju podatke za upotrebu na različitim lokacijama kao što su biblioteke, kampusi, kafeterije, restorani i sl.

3.5. Fizičke i električne karakteristike



Slika 6 - Dimenzije inteligentne kartice

Fizička veličina inteligentnih kartica je dizajnirana kao ID-1 i opisana je standardom ISO 7810. Dimenzije su 85.6 mm sa 54 mm, sa ivicama prečnika 3.18 mm i debljinom 0.76 mm. U vrijeme kada je kreiran ISO 7810 nije se vodilo računa o položaju čipa na ovoj kartici nego samo o položaju ispupčenja, magnetne trake itd. Položaj čipa na inteligentnoj kartici je definisan standardom ISO 7816-2. Fizičke karakteristike su date na slijedećoj slici:

Električne osobine za inteligentne kartice su definisane standardima ISO/IEC 7816-2 i 7816-3 i GSM 11.11. Najčešće inteligentne kartice imaju osam kontaktnih polja na prednjoj strani od kojih su dva rezervisana za buduću upotrebu, tako da neki proizvođači proizvode kartice samo sa šest kontaktnih polja, što blago smanjuje troškove proizvodnje. Električni kontakti su tipično poredani od lijevog vrha na desno i označeni sa C1 do C8.

3.6. Prenos podataka

Sva komunikacija ka i od inteligentne kartice se izvršava preko kontakta C7. Dakle, samo jedna strana može komunicirati u jednom trenutku bilo da se radi o kartici ili terminalu. Ovo se zove poludupleksni prenos. Komunikacija je inicirana od strane terminala što upućuje na tip klijent/server odnosa između kartice i terminala.

Pošto se kartica ubaci u terminal, ona se napaja preko terminala, izvršava *power-on-reset* i šalje 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 fizičke transmisije se definiše standardom ISO/IEC 7816-3. On definiše nivo napona koji se završava prevođenjem u bite 0 i 1.

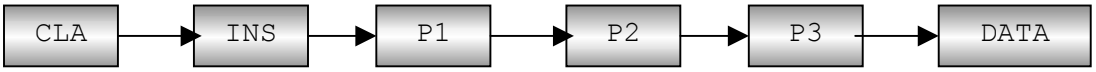
Postoji nekoliko različitih protokola za razmjenu informacija u klijent/server strukturi. Protokoli su prikazani u slijedećoj tabeli:

Protokol	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 10536-4)
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 buduću upotrebu

Tabela 3 - Protokoli za razmjenu informacija u klijent/server strukturi

Najčešće korišteni protokoli su T=0 i T=1. Najpopularniji je T=0 i kratak pregled instrukcija ovog protokola je dat na slijedećoj slici:



Slika 7 - Tipična T=0 instrukcija

3.7. Set instrukcija

Postoje četiri međunarodna standarda koji definišu tipičan set instrukcija za inteligentne kartice. Više od 50 instrukcija i njihovih pripadajućih izvršnih parametara se definišu ovim standardima. Iako se radi o različitim standardima, instrukcije su u mnogome kompatibilne. Standardi su GSM 11.11 (prETS 300608), EN 726-3, ISO/IEC 7816-4 i preliminarni CEN standard prEN 1546. Instrukcije se klasifikuju po funkcijama kao što slijedi:

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

Tabela 4 - Primjer tipova instrukcija

Naravno, inteligentna kartica će koristiti samo podskup mogućih instrukcija potrebnih za datu aplikaciju. Ovo je posljedica ograničenja vezanih za korištenu memoriju i troškove.

3.8. Operativni sistem

Iako sadrže samo nekoliko hiljada bajtova programskog koda, operativni sistem za procesore inteligentnih kartica mora obaviti takve zadatke kao što su:

- prenos podataka preko dvostranog serijskog terminalnog interfejsa,
- učitavanje operacije 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 PC sistema kao što su UNIX, DOS i Windows, operativni sistemi za inteligentne kartice nisu prioritetno orijentisani na korisničke interfejse ili sposobnost da pristupe vanjskim periferijama ili medijima za čuvanje podataka. Veličina je tipično između 3 i 24 kilobajta. Niža granica se tako koristi za specijalizovane primjene, dok je gornji limit vezan za

operativne sisteme u slučaju višestruke primjene inteligentnih kartica. Pošto je memorijski prostor inteligentnih kartica prilično ograničen, ne mogu se sve standardizovane instrukcije i strukture datoteka generalno implementirati u sve operativne sisteme za inteligentne kartice. Iz ovog razloga, uvedeni su u upotrebu tzv. profili, standardima ISO 7816-4 i EN 726-3. Profil definiše minimum zahtjeva za strukturu podataka i komande.

3.9. Vrste napada

Logički napadi

Logički napadi se događaju kada inteligentna kartica radi u normalnim uslovima, ali se dolazi do osjetljivih informacija ispitujući bajte koji dolaze i odlaze od inteligentne kartice. Primjer ovoga napada je tzv. vremenski napad "timing attack", kod koga se različiti uzorci bajtova šalju kartici na potpisivanje pomoću privatnog (tajnog) ključa. Informacija kao što je vrijeme potrebno da se izvrši operacija i broj nula i jedinica u ulaznom bajtu se koristi kako bi se eventualno došlo do tajnog ključa. Postoje logične kontramjere na ove napade , ali mnogo proizvođača inteligentnih kartica ih ne provodi. Ovakav napad zahtjeva poznavanje PIN koda kartice , tako da mnoge operacije vezane za tajni ključ mogu biti izvršene na odabranim ulaznim bajtovima.

Fizički napadi

Fizički napadi se događaju kada se normalni fizički uslovi, kao što su temperatura, frekvencija, napon, itd, mijenjaju, da bi se dobio pristup osjetljivim informacijama na inteligentnoj kartici. Većina operativnih sistema koje koriste inteligentne kartice zapisuju podatke od značaja u područje EEPROM memorije u šifrovanom obliku, tako da je vrlo teško dobiti otvoreni tekst, direktnim hakerisanjem EEPROM-a. Drugi fizički napadi koji su se pokazali uspješnim, uključuju intenzivnu fizičku fluktuaciju u tačno određeno vrijeme i na određenom mjestu, gdje se odvija verifikacija PIN-a. Stoga se mogu izvršavati određene funkcije i bez poznavanja PIN koda. Ovakvi napadi se mogu kombinovati sa logičkim napadima da bi se došlo do tajnog ključa. Većina fizičkih napada zahtijeva posjedovanje posebne opreme.

Trojanski konji

Ovakve aplikacije se pojavljuju i zadržavaju u radnoj stanici neopreznog korisnika. Trojanski konj čeka da korisnik unese važeći PIN kod iz povjerljive aplikacije, omogućavajući upotrebu tajnog ključa i tada poziva inteligentnu karticu da digitalno potpiše neke zlonamjerne kodove. Operacija se završava, ali korisnik nije svjestan činjenice da je njegov tajni ključ upotrebljen mimo njegove volje. Kontramjera koja spriječava ovakve napade je korištenje arhitekture *"single-access device driver"*. Operativni sistem jača, tako da samo jedna aplikacija može pristupiti serijskom uređaju, pa tako i inteligentnoj kartici, u bilo kom trenutku. Još jedan način da se spriječi upad je korištenje modela kojim se dozvoljava upotreba samo jednog tajnog ključa za svaki unos PIN koda. Dakle, kod ovog modela, korisnik mora unijeti svoj PIN svaki put kada se koristi tajni ključ, tako da trojanski konj nema pristup ključu.

Napadi usmjereni na nepažnju korisnika i administratora sistema

U računarskim sistemima, ovaj tip napada se pokazao kao najuspješniji, pogotovo kada je oprema pravilno konfigurisana. Obično se ovi napadi oslanjaju na greške prouzrokovane ljudskim faktorom. Primjer ovakvog napada je kada se napadač izdaje za administratora mreže. On pristupa sistemu i zahtijeva lozinke korisnika za obavljanje različitih aktivnosti u mreži. Korištenjem inteligentnih kartica, otežava se mogućnost ovakvih napada.

Bilo kakav sigurnosni sistem, uključujući i onaj sa inteligentnim karticama, nije potpuno siguran. Uvijek postoji procjena troškova potrebnih za razbijanje određenog sistema, koji bi trebali da budu mnogo veći od vrijednosti podataka koji bi se mogli dobiti razbijanjem sistema. Nezavisne laboratorije vrše ispitivanja na karticama vodećih proizvođača i one mogu izvršiti procjenu troškova u opremi i stručnosti napadača potrebnih za razbijanje sistema. Prilikom izbora inteligentne kartice, kupac ili

korisnik bi trebalo da traži od proizvođača ocjenu od strane nezavisne laboratorije koja je izvršila testiranje sigurnosti. Koristeći ove informacije, teži se tome da se obezbjedi da troškovi razbijanja sistema budu mnogo veći od vrijednosti podataka koji se mogu dobiti neovalaštenim upadom u sistem.

U ovom izlaganju fokusirali smo se na osobine inteligentnih kartica i njihovu ulogu u sistemima za zaštitu računarskih mreža i PC sistema. Kartice su se pokazale kao pogodan medij za obavljanje različitih transakcija, autorizaciju i identifikaciju. Pošto se sposobnosti i mogućnosti ovih kartica povećavaju iz dana u dan, dolazimo u situaciju da jedna kartica može zamijeniti kompletan sadržaj našeg novčanika, uključujući kreditne kartice, vozačku dozvolu, gotovinu, pa čak i porodične fotografije. Sadržavajući različite sertifikate, ove kartice možemo koristiti za identifikaciju, bez obzira gdje se nalazimo i šta želimo da radimo.

3.10. Čitači i terminali

Termin čitač se koristi da opiše jedinicu koja služi kao interfejs sa personalnim računarom za većinu zahtjeva za njegovu obradu. Obrnuto, terminal je samostalan uređaj za obradu. I terminali i čitači mogu čitati i upisivati podatke na inteligentne kartice. Čitači se pojavljuju u različitim oblicima i s različitim sposobnostima. Zato je najlakši način da se opiše čitač po načinu povezivanja sa personalnim računarom. Razlikujemo slijedeće interfejse: RS232 serijski port, USB port, PCMCIA slotovi, floppy disk slot, paralelni port, infracrveni IRDA port, itd.

Pružaje se široke mogućnosti u izboru terminala. Većina njih ima sopstvene operativne sisteme i alate.

3.11. Čitači inteligentnih kartica

Terminali za inteligentne kartice se obično nazivaju čitačima iako, po definiciji, imaju sposobnost čitanja i upisivanja dok god inteligentna kartica podržava taj proces i dok su ispunjeni odgovarajući uslovi pristupa. Za razliku od inteligentnih kartica čija je konstrukcija vrlo slična, čitači inteligentnih kartica se pojavljuju u različitim oblicima sa različitim nivoima mehaničkih i logičkih karakteristika. Neki primjeri uključuju: čitač integrisan u uređaj, ručni akumulatorski čitač sa malim LCD displejom, čitač integrisan u GSM mobilni telefon, čitač priključen na personalni računar ili čitač beskontaktnih kartica čija je struktura data na slijedećoj slici.

Slika 8 - Primjeri čitača inteligentnih kartica

3.11.1. Radna stanica i kontrola pristupa mreži

Čitači inteligentnih kartica koje su prikačene na računare ili montirane na tastaturu omogućavaju korisnicima da pristupe kampus mreži. Korisnici treba da ubace svoje kartice prilikom logovanja. Kada korisnik ubaci karticu sistem čita identifikacioni broj i lozinku sa kartice i prosljeđuje ih u mrežu na autorizaciju. Ovo rješenje ne zahtijeva promjene na serverima za autorizaciju. Administrator domain servera upravlja dozvolama za pristup korisnika kao i obično, bez obzira na to da li se korisnici loguju ručno ili koristeći inteligentnu karticu. Nema potrebe da dodajemo ekstenzije za inteligentne kartice na strani servera. Logovanje pomoću inteligentne kartice i ručno, rade u paraleli. Samo logovanje pomoću inteligentne kartice nudi povećanu bezbjednost i druge pogodnosti:

- korisničko ime (*user name*) i lozinka (*password*) se čitaju sa kartice i prosljeđuju automatski na server, bez djelovanja korisnika,
- koriste složenije lozinke pomoću automatskog slučajnog generisanja,
- nema potrebe za pamćenjem lozinki,
- korisnik ne može dijeliti lozinku sa drugima,
- omogućena je češća izmjena lozinke,
- zaštita od neovlaštenog upada koristeći trostruko DES šifrovanje (*Triple DES Encryption*) i izmjenu ključeva za sesiju (*Session keys*),
- sva prava pristupa su prethodno definisana na mrežnom serveru.