Fakultet elektrotehnike i računarstva
ZESOI

Sustavi za praćenje i vođenje procesa

Seminarski rad

SMART CARD

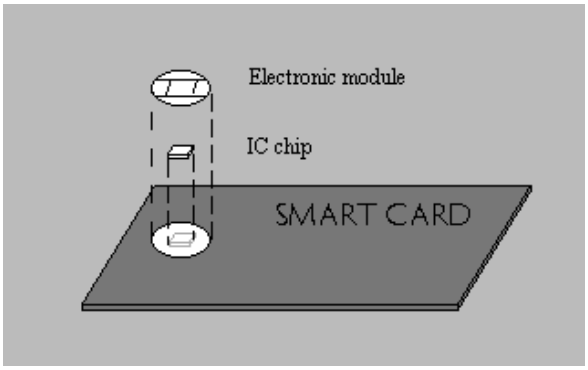
31. svibanj 2004.

Silvije Štuglin
0036386467
Industrijska elektronika

Sadržaj:

1. Uvod

Smart Card ili tzv. 'Pametna kartica' je plastična kartica veličine obične kreditne kartice kakve su nam prisutne u svakodnevnom životu, s tim da u sebi ima ugrađen čip na kojem se nalaze procesor, memorija (RAM i ROM) i sklopovi koji omogućavaju komunikaciju odnosno razmjenu podataka s okolinom. Čip je upravo ono što ove kartice čini pametnima. Ova veza između prikladne plastične kartice i mikroprocesora omogućava nam da se nazamisliva količina podataka može pohraniti, dohvatiti i procesirati bilo online ili offline. Pametne kartice (*Smart Card*) mogu pohraniti nekoliko stotina puta više podataka nego dosadašnje obične kartice s magnetskom trakom. Informacija ili aplikacija pohranjena na čipu u kartici prenosi se pomoću ugrađenog sklopovlja do terminala ili čitača kartice. Bezkontaktne pametne kartice imaju u sebi ugrađenu antenu s kojom bežično komuniciraju s čitačem kartica koji također imaju sličan takav modul, čime se postiže veća komfornost i fleksibilnost. Ovisno o tome kakav je čip ugrađen u karticu razlikujemo dva tipa kartica: *memorijske kartice* i *procesorske kartice*.



Slika 1: Smart kartica – osnovna struktura

Memorijske kartice su one kod kojih je u čip ugrađena samo memorija. Takve memorijske kartice mogu pohraniti i do tisuću puta više podataka od običnih kartica s magnetskom trakom. Zbog sigurnosnih razloga primjena ovakvih kartica ograničena je na one aplikacije kod kojih sigurnost podataka ne igra veliku ulogu. Ovakve kartice obično se koriste u jednostavnim aplikacijama kao što su naprimjer telefonske *čip kartice.*

Procesorske kartice su kartice koje osim memorije na čipu imaju ugrađen mikroprocesor, pa prema tome mogu obavljati različite funkcije kao što su npr. enkripcija podataka, napredna sigurnost podataka (informacije), lokalna obrada podataka, kompleksne operacije nad podacima itd. Zbog svoje velike sigurnosti većina kartica koje sadržavaju povjerljive podatke, su tipa procesorskih pametnih kartica.

Naprimjer pametne kartice mogu biti identifikacijske kartice koje koriste da bi se dokazao identitet vlasnika kartice. Mogu biti zdravstvene kartice na kojima se može čuvati povijest bolesti pacijenta. Nadalje pametna kartica može služiti kao kreditna ili debitna kartica, te se pritom mogu obavljati offline transakcije. Sve ove primjene zahtjevaju sigurnu pohranu podataka kao što su biometrični podaci, povijesti bolesti pacijenta, tajni broj kreditne kartice te razni ključevi za kriptiranu autentičnost.

Smart Card tehnologija je mnogo popularnija u Europi nego u SAD-u. Razlog tome je što se u SAD-u prilično razvila tehnologija koja podržava kartice s magnetskom trakom, te je uloženo mnogo resursa u mreže koje osiguravaju sigurnost transakcija pa se će trebati više vremena da se prijeđe na novu tehnologiju. S druge strane tehnologija kartica s magnetskom trakom nije se razvila dovoljno, umjesto toga kartica nosi svu 'pamet'. U Europi zdravstveno osiguranje i bankarstvo koriste pametne kartice sve intenzivnije. Svaki njemački državljanin koristi Smart Card kao karticu zdravstvenog osiguranja.

Zbog dodane procesorske inteligencije, veličine i mogućnosti obrade podataka, može pružiti veću sigurnost i stoga ima veliku primjenu u različitim područjima. Trenutno se pametne kartice koriste za plaćanje telefonskih poziva, pri plaćanju parkiranja i cestarina, pohranjivanje povjerljivih podataka, za pristup satelitskim televizijskim programima i u mnogim drugim aplikacijama.

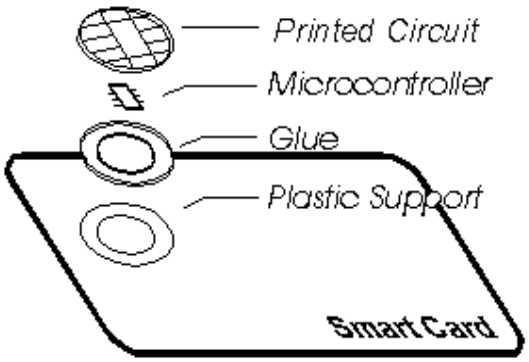
U ne tako dalekoj budućnosti, sve tradicionalne kartice s magnetskom trakom biti će zamijenjene i sve integrirane u jednu jedinu karticu u tzv. multi-aplikacijsku pametnu karticu, koja je u Smart Card riječniku danas poznata pod nazivom elektronička lisnica (E-wallet). Smart kartice postaju sve više značajnije i odigrat će važnu ulogu u našem svakodnevnom životu.

U ovom whitepaperu razmotrit će se osnovni pojmovi i funkcionalnost Smart kartica. Najprije će se razmotriti osnovna fizička struktura kartica, a zatim osnovni dijelovi od koji se ona sastoji. Razmotrit će se tipovi Smart kartica te njihove prednosti i mane. Posebni naglasak dati će se na sigurnost transakcija, što je neophodno za takvo kartično osiguranje. Na kraju predstaviti će se područje primjene i prednosti Smart kartica u odnosu na nesigurne sustave kakve imamo danas.

2. Fizička struktura SMART kartica

Fizička struktura pametne kartice specificirana je od International Standards Organization (ISO). Općenito se sastoji od tri osnovna elementa. Plastična kartica je najosnovniji element i ima dimenzije 85,6 mm×53,98 mm×0,80 mm.

Integrirani čip i kontakti ugrađeni su na karticu. Slika pokazuje pregled fizičke strukture Smart kartice.



Slika 2: Fizička struktura Smart kartica

Kontakti su također propisani ISO standardom i predstavljaju 5 pinsku vezu sa napajanjem i podacima.

Sposobnost pameti kod Smart kartica leži upravo u integriranom krugu. Tipično se integrirani krug sastoji od mikroprocesora, ROM memorije, radne memorije (RAM) i električki izbrisive programabilne ROM memorije (EEPROM) koja će pamtiti svoje stanje i kad napajanja nestane. Čip na kartici napravljen je na siliciju što povlači činjenicu da nije fleksibilan i lako se lomi. Kako se čip nebi uništio prilikom savijanja kartice njegova veličina reducirana je na svega par milimetara.

Općenito, veličina, debljina i fleksibilnost prilikom savijanja dizajnirani su tako da zaštite karticu od fizičkog oštećenja. S druge strane to ograničava veličinu memorije i procesorskih resursa koji su spremljeni na njoj. Zbog ovih ograničenja moraju postojati sklopovi koji se nalaze izvan kartice (npr. u čitaču) npr. napajanje, podaci o vremenu i datumu itd. Ova ograničenja mogu degradirati stupanj sigurnosti jer su obično ti vanjski sklopovi u nekim okolnostima nesigurni i podložni napadima od strane uljeza.

3. Elementi Smart kartica

Smart kartice imaju ista osnovna tri elementa kao i svi ostali računalni sustavi: procesorsku snagu, pohranu podataka i sredstva koja se bave ulazom i izlazom podataka. Procesorska snaga je obično mikroprocesorski chip (npr. Intel 8051 i Motorola 6805), a pohrana podataka izvedena je pomoću memorijskog čipa (EEPROM, FLASH, ROM, RAM). U većini Smart kartica ovi resursi su kombinirani u jedan čip. Prijenos podataka varira od kartice do kartice ovisno o namjeni. Da bi kartica mogla raditi mora imati i izvor napajanja koji je obično čitač kartice ili se pak nalazi na kartici.

➢ Mikroprocesor

Mikroprocesor je inteligentni element Smart kartice koji manipulira podacima i vrši njihovu interpretaciju. Software koji je zadužen za interpretaciju i manipulaciju podacima može biti upisan u memoriju prilikom proizvodnje kartice ili naknadno upisan pod kontrolom mikroprocesora.

Mikroprocesori u Smart karticama mogu biti 16-bitni i raditi na taktu od 10 MHz.

➢ Memorija

Memorija u pametnim karticama može biti ili rijetko promijenjiva (non-volatile), zadržavajući podatke nakon nestanka napajanja, ili promijenjiva (volatile) kod koje podaci nestaju nakon nestanka napajanja. U tom slučaju Smart kartica bi zahtijevala bateriju za napajanje.

Memorija isto tako može biti takva da dozvoljava čitanje iz nje i pisanje u nju (RAM) ili pak samo čitanje iz nje (ROM). U većini slučajeva Smart Card aplikacije zahtijevati će ne promijenjivu memoriju za pohranivanje podataka tipa identiteta vlasnika kartice i aplikacijskog softvera i promijenjivu memoriju za ažuriranje pohranjenih podataka kao što je npr. stanje bankovnog računa nakon transakcije.

Memorije u Smart kartica se stoga mogu kategorizirati u tri skupine: ROM, RAM i programabilni ROM (PROM).

ROM memorija je nepromijenjiva i njen sadržaj je u nju upisan prilikom proizvodnje. Jednom upisan, sadržaj se više nemože mijenjati. U Smart karticama prisutne su memorije od otprilike 32 kB.

RAM memorije su promijenjive i služe samo za privremeno pohranjivanje podataka jer se, kako smo već naveli, podaci nakon nestanka napajanja iz nje brišu. Podaci se u RAM mogu upisivati biti čitani, mijenjani, i brisani. U Smart karticama je raspoloživo 64 kB RAM memorije.

Postoje dvije vrste programabilnih ROM memorija (PROM): električki programabilne ROM (EPROM) i električki izbrisive programabilne ROM (EEPROM) memorije. Za razliku od EPROM-a, EEPROM se može reprogramirati, ali mu je zato struktura mnogo složenija, što ga čini mnogo skupljim. Raspoloživo je oko 8 kB EEPROM memorije.

Memorija može biti struktuirana tako da omogućava različite nivoe zone sigurnosti. Otvorena zona sigurnosti sadrži podatke koji nisu povjerljivi npr. identitet vlasnika. Tajna zona memorije sadrži povjerljive podatke (npr. PIN) te je nedostupna svima osim procesoru koji provjerava taj broj sa brojem koji unosi korisnik. Na taj način povjerljivi podaci nikada ne izlaze iz kartice.

➢ Ulaz/izlaz

Postoji više načina da se podaci prenesu u karticu ili da se iz nje pročitaju. Kontaktne kartice obično sadrže metalne kontakte na površini kartice, koji, kad su ubačeni u čitač, povezuju unutrašnjost kartice sa vanjskim svijetom.

Bezkontaktne kartice koriste neku od bežičnih tehnologija prijenosa podataka, što uvjetuje to da se kartica mora nalaziti u blizini uređaja koji vrši upis/ispis podataka.

Super Smart kartice imaju integriranu tipkovnicu i mali display i prema tome im nije potreban neki uređaj za prijenos podataka, već se podaci mogu unijeti od strane korisnika. Ovakve vrsta kartica ima ipak kontakte koji joj omogućuju da komunicira s drugim uređajima takvoga tipa.

➢ Izvori napajanja

Općenito postoje tri metode napajanja Smart kartica. To su:

- **Iz vanjskog izvora napajanja preko kontakata**

  U ovoj metodi energija je poslana kartici preko dva kontakta koja se nalaze na površini kada se kartica ubaci u uređaj koji zatim vrši pisanje/čitanje podataka. Nakon ubacivanja u uređaj kartica će se sama resetirati (reset on power) i početi izvršavati program u memoriji, koji će početi komunicirati.

- **Iz vanjskog izvora napajanja prijenosom energije**

  U ovoj metodi, bežičnim putem, kao npr. induktivnom vezom, će se prenjeti energija koja će biti dovoljna da pobudi u kartici nekakav proces koji će izvršiti neku kratku operaciju i zatim se ugasiti. Da bi ovo bilo moguće kartica se mora nalaziti u neposrednoj blizini tog uređaja kako bi prijenos energije bio učinkovit.

- **Iz baterije koja je ugrađena u karticu**

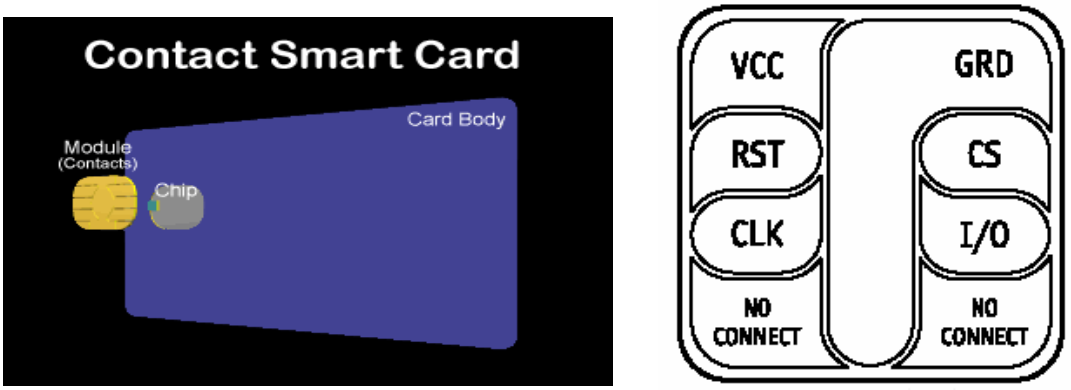
  U ovoj trećoj metodi, baterija je sastavni dio kartice, i kartica se iz nje napaja. Ova metoda nije popularna zbog teškoća koje nastaju u zadovoljavanju ISO standarda, a odnose se na dimenzije, težine, i troškova koji rastu s ugrađivanjem baterije u karticu.

4.Tipovi Smart kartica

Ovisno o tome kako se kartici pristupa, Smart kartice se mogu svrstati u 4 glavne skupine:

➢ Kontaktne Smart kartice

Ove kartice imaju svu mikroelektroniku ugrađenu u unutrašnjost kartice u obliku jednog čipa, veličine oko 10 mm, kojem su zlatni kontakti izvedeni na površinu kartice. Kontakti omogućuju povezanost vanjske jedinice (Smart Card Reader) što omogućuje to da neki uređaj uspostavi komunikaciju i prenese energiju do mikroelektronike u čipu.



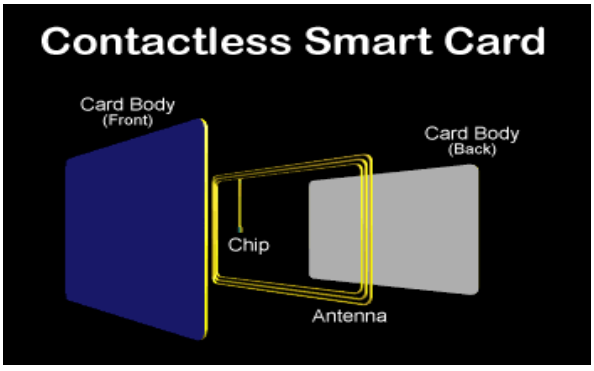
Slika 3 Kontaktna Smart kartica i kontakti

Kontakata ukupno ima 8: Dva su rezervirana za napajanje (VCC, GND), jedan za signal takta (CLK), jedan za reset (RST), dva se koriste za komunikaciju (I/O, CS), a dva su unaprijed rezervirana i ne koriste se. Mnoge kartice imaju još i magnetsku traku na poleđini radi kompatibilnosti s postojećom opremom.

Znači integrirani krug treba napajanje, signal takta koji upravlja procesorom i vezu s koje će primiti odnosno na koju će slati podatke. Kod ove vrste kartica ovo se postiže preko kontakata.

➢ Bezkontaktne Smart kartice

Bezkontaktne Smart kartice imaju ugrađenu neku vrstu antene i umjesto kontaktne veze koriste nekakvu vrstu elektromagnetskog povezivanja. Kako prijenos energije pada s udaljenošću, kartica se mora nalaziti u blizini čitača, na otprilike 3 cm. Induktivna ili kapacitivna veza se koristi kao način prijenosa energije i podataka na karticu. Signal takta može biti interno izveden, a ulazno/izlazna komunikacija se može ostvariti pomoću jedne od vrsta modulacija.



Slika 4: Bezkontaktna Smart kartica

U nastavku će biti opisane prednosti i mane bezkontaktnih kartica u odnosu na kontaktne.

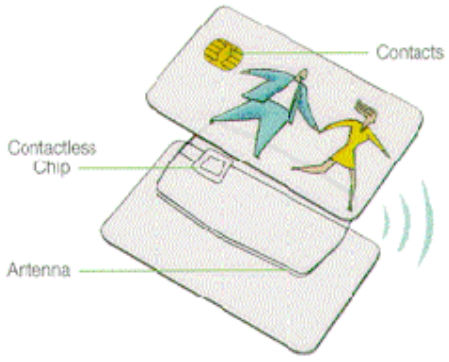
- **Prednosti i mane bezkontaktnih Smart kartica**

Današnje bezkontaktne Smart kartice su definirane relativno lošim standardom, jer različiti proizvođači koriste različite metode prijenosa podataka i energije koje su nekompatibilne jedna s drugom. Bezkontaktne kartice mogu biti relativno spore i skupe za izradu i mogu prestati s radom prilikom savijanja jer za razliku od kontaktnih kartica nisu napravljene od jednog čipa već od većeg broja povezanih komponenti. Sa strane sigurnosti bezkontaktne kartice su manje sigurne zbog mogućnosti da uvijek može postojati još neko tko sluša sve što mi šaljemo te to može zlouporabiti.

Međutim bezkontaktne Smart kartice imaju i svojih prednosti:

- **Pouzdanost i dulji životni vijek:** Površinski kontakti su najčešći kvarovi koji se događaju u elektroničkim sustavima ovoga tipa. Površinski kontakti su stoga podložni oštećenju i onečišćenju što gotovo sigurno uvjetuje kvar sustava.
- **Orijentacija:** Bezkontaktna kartica može biti u bilo kojoj orijentaciji u odnosu na čitač, za razliku od kontaktne koja se mora gurnuti u za to predviđen utor, i imati pritom određenu orijentaciju.
- **Prikladnost:** Jedinica koja čita/piše na karticu može biti ugrađena u bilo kakvo nemetalno kučište, što omogućuje bolju mehaničku zaštitu takve jedinice.
- **Minimalno održavanje:** Ne postoje nikakvi pokretljivi mehanički dijelovi što uvjetuje minimalno održavanje takvih sustava.
- **Robusnost:** Čitači i bezkontaktne kartice mogu podnijeti gotovo bilo kakve uvjete okoline kao i vremenske uvijete. Zbog toga su prikladne za industrijsku ili neku sličnu okolinu gdje mogu doći u doticaj s uljem, masnoćom ili prašinom.

➢ CombiCard



Slika 5: CombiCard

Combi Card je kombinacija kontaktnih i bezkontaktnih kartica spojenih u jednu karticu te se time ostvaruje primjenjivost Smart kartica na gotovo bilo koji sustav. Ova kartica ima još i kao dodatak magnetsku traku sa strane te dvodimenzionalani ili jednodimenzionalni bar kod, pa je prema tome kartica multiaplikacijska i primjenjiva na postojeće sustave.

➢ Super Smart Card

Slika 6: Super Smart Card

Tipovi Smart kartica koji su opisani do sada bili su pasivni tipovi kartica koji su zahtijevali vanjski izvor napajanja i terminal koji je vršio upis i ispis podataka. Ovo ograničenje neizbježno utječe na prikladnost primjene u određenim aplikacijama. Npr. svaki pasivni sistem Smart kartica mora osigurati raspoloživost terminala u planiranom području primjene. Ovo je dovelo do razvoja treće generacije aktivnih Smart kartica poznatih pod nazivom Super Smart kartice.

Super Smart karice sadrže tipkovnicu i LCD display direktno na površini kartice. Ovakva kartica može biti potpuno samostalna (standalone) jedinica ili se pak može priključiti na računalo, iz čega možemo zaključiti da ima i površinske kontakte koji joj to omogućavaju.

Mane ovakvih tipova kartica je visoka cijena proizvodnje u usporedbi s drugim Smart karticama, problemi koji se javljaju u zadovoljavanju ISO standarda i relativno mala veličina ugrađene tipkovnice.

Primarna pogodnost Super Smart kartica je mogćnost offline rada i samoprovjeravanja. Za razliku od terminalno ovisnih pasivnih kartica Super Smart kartica se može korisiti na bilo kojem mjestu i bilo koje vrijeme.

5.Sigurnost Smart kartica

Sigurnost je jedno od najvažnijih obilježja Smart kartica. To je često primarna važnost, posebno kod financijskih aplikacija, i kada je u pitanju privatnost podataka. Za razliku od pasivnih sustava, kao što su npr. kartice s magnetskom trakom, Smart kartica kao primjer aktivnog sustava, sa svojom ugrađenom inteligencijom, sposobna je pretrpjeti razne napade od strane neautoriziranih osoba koje imaju namjeru prijevare ili pak čitanja povjerljivih podataka spremljenih na kartici.

S druge strane za Smart kartice nemože se tvrditi da su 100% sigurne. Svaki sistem može se ugroziti uz dovoljnu količinu resursa koji je potrebno uložiti da bi se to ostvarilo. Sada, da li će se sistem moći ugroziti ovisi ustavari o tome da li se to isplati učiniti, tj. da li je razina sigurnosti veća od razine truda i resursa koji bi trebalo uložiti da bi se ona ugrozila.

Ali činjenica stoji, da Smart kartice pružaju više sigurnosti nego obične kartice s magnetskom trakom ili bilo koji široko upotrebljiv sustav današnjice. Gotovo svi napadi na Smart kartice u zadnje vrijeme klasificirani su kao napadi 3. stupnja, što znači da su potrebni milijuni dolara, i stotine godina računalne snage, da bi se ustvari ugrozila sigurnost jedne transakcije.

➢ Mehanizmi sigurnosti podataka

- **Integritet podataka**

  Ovo je funkcija sigurnosti koja provjerava određene karakteristike dokumenta i transakcije. Ovaj mehanizam osigurava da podaci nisu prilikom prijenosa koruptirani ili izgubljeni. Karakteristike dokumenta i transakcije provjeravaju se kako bi se utvrdila točnost podataka i pravilna autorizacija. Integritet podatak se postiže elektroničkom kriptografijom koja dodjeljuje jedinstveni identitet podacima kao npr. otisak prsta. Na taj način promjena tog identiteta signalizira neku promjenu i na taj način se može znati da li su podaci bili podloženi promjeni.

- **Autentičnost**

  Ovaj mehanizam prvo ispituje, a zatim potvrđuje pravilan identitet *'osoba'* koje sudjeluju u transakciji podataka. Digitalni potpis (Digital Signature) provjerava podatke i njihovo porijeklo i procesira identitet koji uzajamno mogu provjeriti sve strane koje sudjeluju u transakciji. Digitalni potpis procesira se pomoću kriptografskog *Hash algoritma, a* temelji se na faktorima velikih primarnih projeva.

- **Nerazdvojivost**

  Ovaj mehanizam eliminira mogućnost razdvojivosti ili dodavanja digitalnog potpisa u poruku, kojeg bi druga strana proglasila točnim.

- **Autorizacija**

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

- **Povjerljivost / Kriptografija**

Povjerljivost je mehanizam koji koristi postupak kriptografije kako bi se zaštitila informacija od neautoriziranog pristupa. Npr. običan tekst je pretvoren u šifrirani oblik pomoću nekog algoritma, a zatim odšifriran u običan tekst istim postupkom.

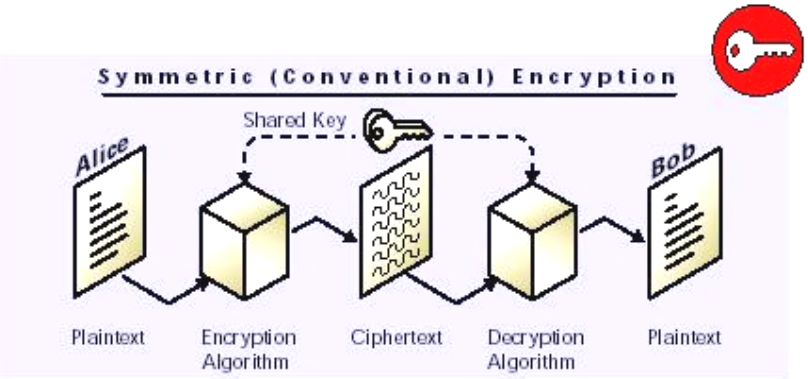
Kriptografija je metoda pretvorbe podataka iz oblika koji je čitljiv ljudima u neki drugi oblik, a zatim natrag u njegov originalni čitljiv oblik, kako bi se otežao pristup neovlaštenim osobama.

Kriptografija se koristi u sljedećim slučajevima:

- U osiguravanju privatnosti podataka, kriptiranjem podataka
- U osiguravanju integriteta podataka, prepoznavanjem da li su podaci bili podvrgnuti neovlaštenom postupku.
- U osiguravanju jedinstvenosti podataka, provjeravanjem da li je poruka originalna ili je kopija originala. Pošiljatelj u originalnu poruku dodaje neki jedinstveni identitet, koji primatelj zatim provjerava.

Originalni podaci mogu biti obliku koji je čitljiv ljudima, kao npr. tekst datoteka, ili u obliku koji prepoznaju računala, kao npr. baza podataka, tablica ili slika. Originalni podaci se nazivaju **nekriptirani podaci** ili **običan tekst**. Podaci koji su podvrgnuti postupku kriptografije nazivaju se **kriptirani podaci** ili **šifriran tekst**. Proces koji pretvara podatke u kriptirane naziva se **enkripcija**, a obrnuti postupak ,dakle pretvaranje kriptiranih podataka u originalni oblik naziva se **dekripcija**.

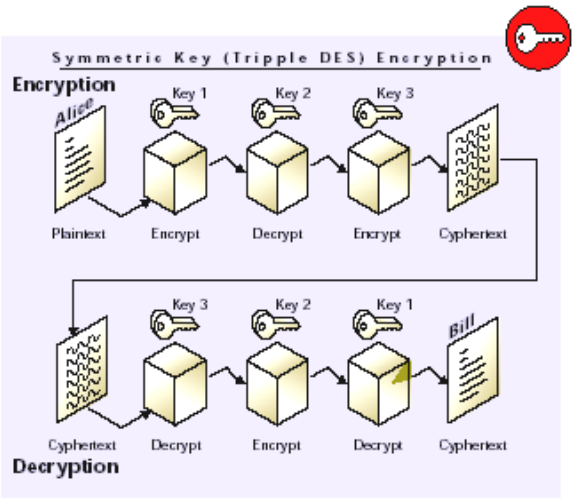
Da bi se podaci mogli pretvoriti iz jednog oblika u drugi, potrebno je imati enkripcijski algoritam i ključ. Ako je isti ključ korišten za enkripciju i dekripciju, on se naziva **simetrični ključ**, a algoritam je prema tome **simetrični**. Najpoznatiji simetrični algoritam je **DES (Data Encryption Standard)**.



Slika 7: Simetrični DES enkripcijski algoritam

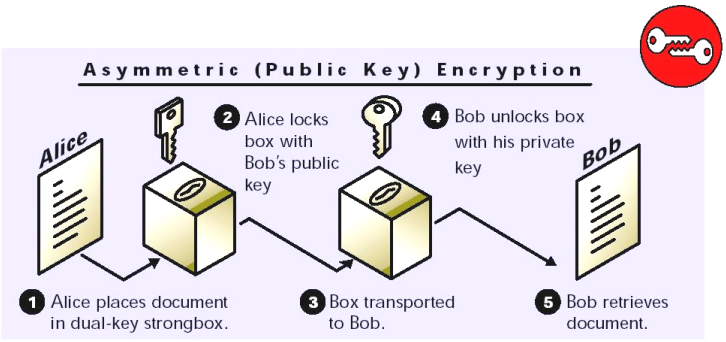
DES simetrični algoritam bio je izumljen u IBM-u 1970. god. Ovaj algoritam je bio proučavan od strane kriptografa više od 20 godina, i za to vrijeme nije bilo nikakvih metoda koje bi omogućile probijanje ove kriptografije. DES algoritam ima 56-bitni ključ, koji omogućuje $2^{56}=7\times10^{16}$ mogućih varijacija. Kod simetrične enkripcije podataka problem predstavlja razmjena ključeva koji se koriste za enkripciju i dekripciju podataka. Kako se za oba postupka koristi isti ključ, pošiljatelj poruke mora primatelju poslati ključ s kojim je poruka enkriptirana. Ako je taj ključ slan preko mreže to ugrožava sigurnost komunikacije.

Trostruki DES (Triple-DES) metoda enkripcije koristi postojeći DES algoritam na poseban način kako bi se poboljšala sigurnost. Trostruki DES algoritam može biti izveden s dva ili tri ključa, ovisno o primjeni. Kako algoritam obavlja enkripciju-dekripciju-enkripciju, često se naziva EDE algoritam. Slika pokazuje princip enkripcije trostrukim DES algoritmom.



Slika 8: Trostruki DES enkripcijski algoritam

Ako su različiti ključevi korišteni za enkripciju i dekripciju, algoritam se naziva **asimetrični algoritam**. Asimetrična enkripcija ima par ključeva, pri čemu se jedan ključ koristi za enkripciju, a komplementaran ključ iz para se koristi za dekripciju. Na taj način svaki korisnik može objaviti jedan ključ (naziva se **javni ključ**), a drugi ključ ostaje poznat samo njemu (**tajni ključ**). Kada pošiljatelj želi poslati poruku može je enkriptirati javnim ključem primatelja poruke. Tada poruku može pročitati samo primatelj kome je namjenjena, a sigurnost ključa nije upitna jer se tajni ključ ne šalje mrežom. Unatoč ovoj očiglednoj sigurnosnoj prednosti, asimetrična enkripcija se rijetko koristi jer je algoritam puno sporiji od simetrične ankripcije. Najpoznatiji asimetrični algoritam je **RSA**, nazvan po svoja tri autora (Rivest, Shamir i Adleman). Na slici je prikazan princip asimetričnog algoritma enkripcije.



Slika 9: Asimetrični enkripcijski algoritam

Kako bi imali prednosti oba sustava (simetričnog i asimetričnog), moderni sigurnosni mehanizmi koriste simetričnu enkripciju za enkriptiranje dokumenata. Enkripcija koristi slučajno generiran ključ koji se tada enkriptira asimetričnim algoritmom i šalje zajedno s porukom. Na taj način je ključ zaštićen a dokument se može dekriptirati bržim algoritmom.

- **Digitalni potpis**

Sustavi opisani u predhodnom poglavlju (kriptografija) omogućuju i digitalni potpis dokumenta. Za digitalni potpis se najprije generira **hash sažetak** dokumenta. Hash sažetak je kratak niz koji jednoznačno definira dokument iz kojeg je nastao. Naime, nemoguće je (barem današnjim tehnikama kriptoanalize) iz poznatog hash sažetka generirati izvorni dokument i nemoguće je kreirati dva različita dokumenta koji bi imali isti hash sažetak. Hash sažetak se još naziva i digitalni otisak poruke jer primatelj može usporediti hash sažetak koji je primio zajedno s porukom i hash sažetak koji je sam generirao iz primljenog dokumenta, te zaključiti da li je dokument izvoran, tj. da li je promijenjem negdje duž komunikacijskog kanala.

Digitalni potpis dokumenta je njegov hash sažetak enkriptiran tajnim ključem pošiljatelja. Primatelj poruke može primljeni potpis dekriptirati javnim ključem pošiljatelja koji mu je dostupan te dobiveni sažetak usporediti s hash sažetkom koji je generirao iz primljenog dokumenta. Ako su sažeci jednaki onda je sigurno da ga je poslao deklarirani pošiljatelj i dokument sigurno nije u međuvremenu promijenjen.

➢ Ugrožavanje sigurnosti

Da bismo predočili veličinu i kompleksnost traženja ključa, tj. probijanje sigurnosnog mehanizma enkripcije navesti ćemo neke ilistrativne podatke.

Ključevi koji se koriste mogu biti (ovisno o algoritmu) dugački od 40 bita za neke manje sigurne aplikacije, pa do 128 bita za aplikacije koje zahtijevaju velik stupanj sigurnosti. Kod 128-bitnog ključa imamo 2^{128} mogućih ključeva. To je u decimalnom zapisu:

3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000,000

U tablici su prikazana estimirana vremena koja su potrebna za probijanje ključa:

Tablica 1: Aproksimativna vremena probijanja ključa

Duljina ključa	Broj mogućih ključeva	Vrijeme za dekripciju uz brzinu 1 enkripcija/1μs	Vrijeme za dekripciju uz brzinu 10^6 enkripcija/1μs
32 bita	$2^{32} = 4{,}3\times10^{9}$	2^{31} μs = 36 minuta	2 ms
56 bita	$2^{56} = 7{,}2\times10^{16}$	2^{56} μs = 1142 godine	10 sati
128 bita	$\mathbf{2^{128} = 3{,}4\times10^{38}}$	$\mathbf{2^{128}}$ **μs =** $\mathbf{5\times10^{24}}$ **god.**	$\mathbf{5\times10^{18}}$ **godine**

6. Prednosti Smart kartica

U usporedbi s uobičajenim uređajima kao što su kartice s magnetskom trakom, Smart kartice nude, poboljšanu sigurnost, prikladnost i ekonomske pogodnosti. Uz to sustavi sa Smart karticama imaju visok stupanj podešavanja, sukladno individualnim potrebama.

- **Sigurnost**

  Smart kartice koriste spoj enkripcije koje mogu obavljati izdavačke i korisničke zahtjeve s najvećim stupnjem sigurnosti. Koristeći enkripciju, podaci mogu biti sigurno prenešeni preko običnih ili wireless mreža. U spoju s biometričkim metodama identifikacije (npr. otisak prsta), Smart kartice se koriste za distribuciju državnih sredstava tamo gdje je to potrebno, reducirajući tako mogućnost zloupotrebe i prijevare. Smart kartice zdravstvenog osiguranja omogućuju doktorima i osoblju pristup pacijentovoj povijesti bolesti, bez ugrožavanja privatnosti.

- **Prikladnost**

  Jedna od prednosti Smart kartica je što će zamijeniti različite identifikacijske kartice. Smart kartice će kombinirati papirnate, plastične i magnetske kartice koje su bile korištene za identifikaciju, kartice koje dozvoljavaju kopiranje, naplatu cestarine, naplatu telefonskih razgovora u telefonskim govornicama, mirovinske i zdravstvene podatke. Sveučilišta, poduzeća i vladine udruge se oslanjaju na Smart identifikacijske kartice jer sadrže mnogo detaljnije podatke i omogućuju integraciju mnogih aplikacija i usluga. Zdravstvo npr. smanjuje troškove obrade baze podataka svih pacijenata, tako da omogućuje pristup osobnim podacima pacijenta koji su pohranjeni direktno na Smart kartici. Kartice na sveučilištima koriste se za plačanje hrane i troškova fotokopiranja.

- **Ekonomske pogodnosti**

  Smart kartice smanjuju troškove transakcija tako što eliminiraju papir i troškove obrade podataka na papiru u bolnicama i državnim službama. Kontaktne i bezkontaktne Smart kartice omogućuju modernizaciju sustava za naplatu cestarine, tako što smanjuju troškove radne snage kao i kašnjenja koja uzrokuju postojeći sistemi. Troškovi održavanja za benzinske crpke, naplatu parkiranja i naplatu telefonskih razgovora su smanjeni, dok prihodi mogu porasti i do 30%, zbog primjene Smart kartica u sustavima plaćanja.

- **Svestranost**

  Smart kartice sadrže sve podatke potrebne osobni pristup mreži, pristup Internetu, plaćanje i druge aplikacije. Koristeći Smart karticu, moguće je uspostaviti osobnu vezu s mrežom bilo gdje u svijetu koristeći se telefonom ili informacijskim kioskom. Web serveri će provjeriti korisnički identitet i predstaviti web stranicu, e-mail ili bilo koji drugi web servis na osnovi podataka pročitanih sa kartice. Osobne postavke potrebne za elektronsku primjenu biti će radije spremljeni na karticu nego u aplikacijama. Telefonski brojevi su spremljeni na kartici, a ne u telefonu. Dok se aplikacije mijenjaju, korisnik nosi sve na kartici koristeći ju kao osnovni mrežni i računalni uređaj.

7.Zaključak

U ovom whitepaper-u je opisana struktura Smart kartica te glavni načini njihove primjene. Smart kartice omogućavaju izgradnju sustava za autentikaciju korisnika s dosad nezamislivom razinom modularnosti, samostojnosti, sigurnosti, nadogradivosti, jednostavnosti i funkcionalnosti.

Smart kartice imaju sve širu primjenu i sve više zamijenjuju stare kartice s magnetskom trakom. U mnogim zemljama zapadne Europe već postoje sustavi poput zdravstvenog osiguranja koji su bazirani na Smart karticama.

Uskoro vjerojatno možemo očekivati univerzalne Smart kartice koje će biti osobna iskaznica, zdravstvena kartica, kreditna kartica, vozačka dozvola, kartica za korištenje mobilnih i bankomat uređaja, kartica za pristup sigurnim mrežnim servisima, ulaznica za knjižnicu i videoteku te još mnogo toga.

Na kraju je zaključeno da je Smart kartica izuzetno siguran uređaj. To je sigurno mjesto za pohranu vrijednih podataka kao što su privatni ključevi, brojevi računa i vrijedni osobni podaci kao što su npr. biometrične informacije. Smart kartica je isto tako sigurno mjesto za obavljanje tzv. offline procesa kao što je enkripcija i dekripcija javnog ili privatnog ključa. Smart kartica može biti element rješenja sigurnosnih problema u modernom svijetu.