# IDENTIFIKACIJA KORISNIKA NA INTERNETU

Tema 4

## Potrebna tehnologija

- Identifikaciona tehnika
- Zakonska regulativa
- Sertifikaciono tijelo
- Zakon o digitalnom potpisu

## Sistemi identifikacije u E-komercu

- Identifikacioni sistemi služe da prepoznaju korisnika i omoguće ostvarenje njegovih prava i obaveza.
- Postoji mnogo vrsta identifikacionih sistema. Neki se zasnivaju na čitanju kontaktne kartice, a neki pomoću radio-talasa (RFID sistemi) razmjenjuju podatke sa korisnikom bez direktnog kontakta. Postoje i biometrijski identifikacioni sistemi koji identifikaciju vrše na osnovu prepoznavanja fizičkih ili karakteristika ponašanja čovjeka (prepoznavanje otiska prsta, dužice oka, lica, glasa i slično).

## PREGLED IDENTIFIKACIONIH TEHNIKA

- Postojeće identifikacione tehnike se mogu podijeliti u dvije osnovne grupe:
  - Tradicionalne identifikacione tehnike i
  - Biometrijske identifikacione tehnike.
- U tradicionalnim identifikacionim tehnikama, objektu čije se prepoznavanje vrši, dodjeljuje se neki identifikator.
- U biometrijskim identifikacionim tehnikama prepoznavanje čovjeka vrši se na osnovu njegovih jedinstvenih fizičkih i/ili karakteristika ponašanja.

## PREGLED IDENTIFIKACIONIH TEHNIKA

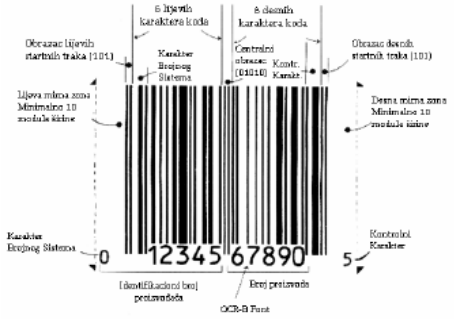
- Najčešće korištene tradicionalne identifikacione tehnike kao identifikator upotrebljavaju:
  - Trakasti kod - BAR COD,
  - Magnetski zapis,
  - ″Pametni″ identifikator.
- Tradicionalni identifikacioni sistemi se upotrebljavaju za identifikaciju predmeta, životinja i ljudi. Svaki objekat, u ovim sistemima, mora posjedovati identifikator. Identifikator može biti različitog oblika i dimenzija. U identifikaciji proizvoda u maloprodaji, identifikator sa trakastim kodom štampa se na omotu proizvoda


Slika 1.1 Trakasti kod oštampan na prozvodu

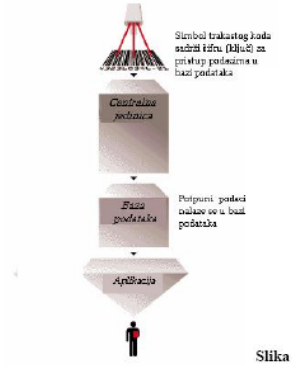
- Trakasti kod je jedan od prvih načina predstavljanja informacija u mašinski čitljivom obliku. Njime se vrši razmjena podataka, svedenih na štampani oblik. Kompjuter generiše štamapnu sliku simbola trakastog koda na papiru ili drugom grafičkom medijumu. Ovaj simbol se zatim prezentuje čitaču trakastog koda. Čitač osvjetljava simbol trakastog koda i ispituje segment po segment u simbolu, da bi odredio da li je visoke refleksije ( međuprostor) ili niske refleksije (traka). Na osnovu toga čitač konvertuje simbol trakastog koda u digitalni signal.

- Ideja primjene trakastih kodova u sistemima za identifikaciju proizvoda u maloprodaji pojavila se već četrdesetih godina prošlog vijeka.
- U dvadesetom vijeku došlo je do prave ekplozije u smislu porasta količine i raznovrsnosti roba kojom se trguje. To je uzrokovalo da cijene logistike i kontrole inventara višestruko naraste, naročito u supermarketima. Zato su oni među prvima dali podršku razvoju sistema za automatsku identifikaciju proizvoda.
- Krenulo se sa stanovišta da bi jednostavna oznaka, mašinski čitljiva, omogućila trgovcima da saznaju sadržaj paketa proizvoda bez potrebe za pojedinačnom provjerom svakog paketa. Mogućnost da se brzo odredi sadržaj paketa ubrzala bi razmjenu robe i smanjila troškove transporta, kontrole inventara i logistike.

- Universal Product Code-UPC je linearan (jednodimenzioni), trakasti kod. (Slika 1.4).




**Slika 1.4.** Kompletan simbol U.P.C koda – verzija A




**Slika 2.1.61** Uobičajeni izgled CCD čitača

**Slika 2.1.30** Jednodimnzioni trakasti kod i aplikacija na PC-u.

**Slika 2.1.50** Čitač sa prorezom ZB-600, proizvod firme ZEBEX

- Druga faza razvoja trakastih kodova ogleda se u pojavi dvodimenzionalnih i matričnih kodova. Dvodimenzionalni i matrični kodovi omogućavaju smještanja više podataka na manjoj površini. Često se koriste za označavanje proizvoda malih dimenzija, kao i tamo gdje je na maloj površini potrebno smjestiti više podataka (npr. audio zapis na filmskim trakama)

**Slika 2.1.32** Code16K simbol

**Slika 2.1.38** Data Matrix simbol


**Slika 1.2** Različite identifikacione kartice

•U slučaju identifikacije čovjeka, identifikator je često standardnog oblika kartice (Slika 1.2).

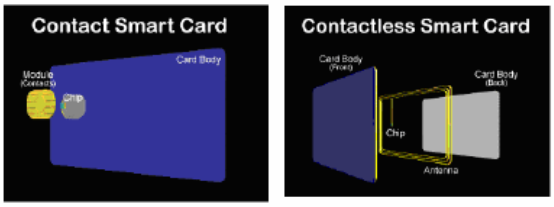
- Danas svuda prisutne, magnetne trake, prvi put su se pojavile ranih 60- tih godina kao prevozne karte u londonskom metrou. Rukovodstvo londonskog prevoza je obložilo zadnju stranu vozne karte, magnetskim zapisom koji je sadržavao šifriranu vrijednost karte. Svaki put kada bi kartica bila provučena kroz čitač na prevoznoj stanici, na magnetsku traku se upisivala nova šifrirana vrijednost koja je u odnosu na raniju umanjena za cijenu prevoza. Sistem je kasnije prerađen. Reduciran je prostor sa magnetskim zapisom na standardni format trake (Slika 1.5)
- Kartice sa magnetnim zapisom (magnetne trake) i dalje se široko koriste kao finansijske kartice, prevozne karte i identifikacione kartice. Pod finansijskim karticama podrazumijevaju se kreditne i debitne kartice, koje se koriste kod automatskih blagajni i terminala na prodajnim mjestima.

**Slika 1.5** Kartica sa magnetskim zapisom oblika trake i čitač Mini123 MSR500m(ur)

- Prevozne karte sa magnetskim zapisom koriste se u gotovo svim vidovima saobraćaja (željeznici, autobuskom saobraćaju, avionskom saobraćaju itd.).
- Magnetni zapis kao identifikator se koristi kod vozačkih dozvola, članskih karata, kartica ključeva i slično

## ″Pametni″ identifikatora

- Identifikacioni sistemi zasnovani na primjeni ″pametnih″ identifikatora sve su prisutniji u našoj svakodnevici. ″Pametni″ identifikatori imaju ugrađen jedan ili više mikročipova. Čip može sadržati mikroprocesor sa internom memorijom ili može biti samo memorijski.
- Prema načinu na koji komuniciraju sa čitačem ″pametni″ identifikatori mogu biti kontaktni ili bekontaktni. Na slici 2.5 prikazan je kontaktni i bezkontaktni identifikator oblika kreditne kartice




Slika 1.5 Kontaktne i beskonraktne (RF) kartice

"Pametne" identifikatore karakteriše visoka zaštićenost podataka. U samom čipu ugrađene su funkcije zaštite. Imaju inteligentnu interakciju sa čitačem.

Identifikacioni sistemi zasnovani na "pametnim" identifikatorima danas ubrzano dobijaju na popularnosti i sve više potiskuju druge tradicionalne identifikacione sisteme. Koriste se širom svijeta u finasijskum poslovima, telekomunikacijama, tranzitu, maloprodaji, zdravstvu, kontroli pristupa itd.

## Biometriski identifikacioni sistemi

- Koriste se za identifikaciju čovjeka na osnovu prepoznavanja njegovih fizičkih karakteristika ili karakteristika ponašanja.
- Kod ovih sistema nije potreban dodatni identifikator, već je on sastvani dio čovjeka.
- Danas postoje biometrijski identifikacioni sistemi koji identifikaciju vrše na osnovu prepoznavanja:
  - otiska prsta,
  - dužice oka,
  - mrežnjače oka,
  - karakteristika lica,
  - karakteristika glasa,
  - karakteristika šake,
  - potpisa, itd.

| Biometrija | |
|---|---|
| Fizičke karakteristike | Ponašanje |
| Otisak prsta | Prepoznavanje glasa |
| Prepoznavanje lica | Potpis |
| Geomatrija šake | Način hodanja |
| Skenir. dužice oka | |
| Skeniranje mrežnjače | |
| DNA | |
| Vaskularni obrasci | |

Biometrijski sistemi se mogu podijeliti u dvije osnovne kategorije i to:
- sistemi zasnovani na prepoznavanju fizičkih karakteristika i
- sistemi zasnovani na prepoznavanju karakteristika ponašanja.

Biometrijske identifikacione tehnike koje su u tabeli ispisane tamnijom bojom, danas se najviše koriste i u njihov razvoj ulažu se najveći napori

# RFID TEHNOLOGIJA

- Radio frekvencijska identifikacija, ili RFID, je opšti naziv za tehnologije koje koriste radio talase za automatsku identifikaciju ljudi ili objekata. To je tehnologija koja se u poslednje vrijeme snažno razvija, i nalazi brojne primjene u svakodnevnom životu.
- RFID tehnologija omogućava identifikaciju uz minimum napora korisnika. Korisnici se mogu identifikovati bez potrebe da pronalaze identifikator (karticu) u svojoj tašni ili novčaniku. Dovoljno je da se kartica nađe u polju čitača i indentifikacija je obavljena. Bezkontaktna razmjena podataka doprinosi da radni vijek RF čitača i RF identifikatora bude duži nego što je slučaj sa čitačima i identifikatorima drugih tehnologija.

# RFID TEHNOLOGIJA

U RFID sistemima:

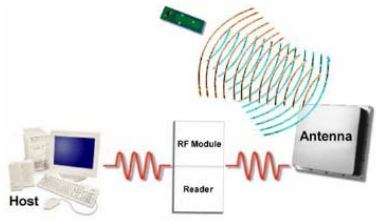
- nema oštećenja kontakata kao kod sistema sa kontaktnim karticama,
- nema oštećenja glave čitača kao kod sistema sa magnetskim karticama,
- nema problema sa prljavštinom i ogrebotinama kao kod sistema sa bar kodom i magnetskim zapisom.
- RF čitač i RF identifikator su otporniji na sabotažu.

- Zahvaljujući prenosu podataka putem radio frekvencija, nije potrebna direkna vidljivost između čitača i RF identifikatora. Ovakvu osobinu ne posjeduje ni jedna do sada razvijena identifikaciona tehnologija

RF čitač i RF identifikator komuniciraju putem RF signala.

Kompletan RFID sistem, u najkraćem, funcioniše na sljedeći način:

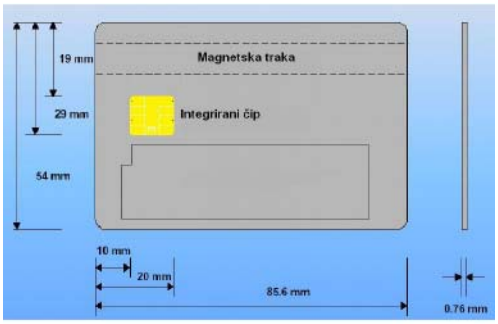
- Čitač generiše elektromagnetni talas.
- Antena RFID taga podešena je da prima ove talase.
- Pasivni RFID tag crpi snagu iz polja čitača i koristi je za napajanje mikročipa.
- Čip moduliše talase, koje tag šalje nazad ka čitaču.
- Antena čitača prihvata modulisani signal.
- Čitač dekodira podatke.
- Izvještaj se šalje host-u.




**Slika 3.1.1** Osnovni sastavni djelovi RFID sistema

# PAMETNE KARTICE

- Pametne kartice se definišu kao kartice standardne veličine koje imaju ugrađen čip i mogu obrađivati informacije (Slika 4.1.1). Time se podrazumijeva da katica može primati, memorisati, obrađivati i odašiljati podatke. Poseban naglasak stavlja se na sigurnost podataka i brzinu obrade kritpografskih funkcija.
- Pametne kartice se još nazivaju i čip kartice ili ICC (Integrated Circuit Card).



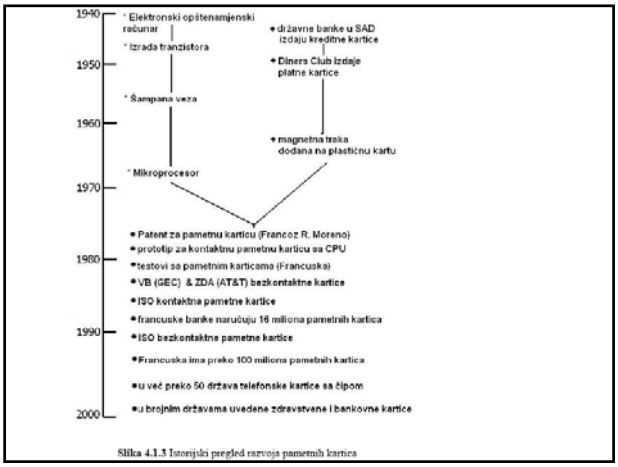

Slika 4.1.1 Standardne dimenzije pametne kartice

- "Pametne" kartice su prvi predložili njemački naučnici Helmut Gröttrup i Jürgen Dethloff in 1968. Patent je prihvaćen 1982.
- Prva masovna upotreba pametnih kartica bila je 1983 godine u Francuskoj. Pametne kartice su upotrijebljene za bezgotovinsko plaćanje telefonskih razgovora.
- 1974. godine Roland Moreno predlaže svoj prvi koncept memorijske kartice. Prvu mikroprocesorsku pametnu karticu predlaže Michel Ugon iz Honeywell Bull-a, 1978 godine. Bull je patentirao SPOM (Self Programmable One-chip Microcomputer) koji definiše neophodnu arhitekturu za auto-programiranje čipa. Tri godine kasnije, prvi "CP8" zasnovan na ovom patentu proizveden je od strane Motorole. Danas, Bull ima 1200 patenta vezanih za pametne kartice.
- Druga velika primjena bila je 1992. godine, takođe u Francuskoj. Ovom primjenom je u sve debitne kartice u Francuskoj ugradjen je čip (Carte Bleue –Slika 4.1.2)


Slika 4.1.2 Carte Bleue

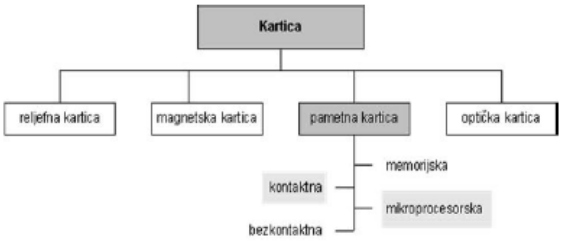
Tokom 1990-ih širom Evrope pojavljuju se sistemi u kojima se ″pametne″ kartice koriste kao elektronski novac. U ovim sistemima podatak o količini novca čuva se na kartici a ne na nekom spoljašnjem računu.

Glavnu primjenu ″pametne″ kartice dobijaju, tokom 1990-ih u mobilnoj telefoniji, kroz uvođenje SIM kartica.
1993. godine MasterCard i VISA prihvatili su uvođenje čipa u njihove kreditne i debitne kartice. Prva verzija EMV (Europay, MasterCard and VISA) sistema pojavlila se 1994. godine. Kanije su uslijedile novije savršenije verzije. Danas, EMV je standard za upotrebu IC kartice i IC kompatibilnih POS terminala




Slika 4.1.3 Istorijski pregled razvoja pametnih kartica

# VRSTE PAMETNIH KARTICA




U mnogim sistemima, u kojima se koriste identifikacione kartice, postoje tri nivoa provjere identiteta.
Jedan nivo je - "**ono što posjeduješ**" a to je kartica, token
Drugi nivo je- "**ono što znaš**", a to je, najčešće, PIN kod, password, odnosno lozinka.
Treći nivo je– "**ono što jesi"**, a to je biometrija

- Pametna kartice, jedine su u stanju primati, obrađivati i slati podatke. One omogućavaju i vrlo jednostava postupak izmjene i brisanja iz svoje memorije, postojećih podataka, daleko fleksibilnije nego bilo koje druge identifikacione kartice.
- Sa stanovišta razmjene podataka sa okruženjem, pametne kartice se mogu podijeliti na:
  - kontaktne,
  - bezkontakne,
  - hibridne i
  - i kartice sa dvostrukim interfejsom (dual interfejs cards) (Slike 4.2.2).



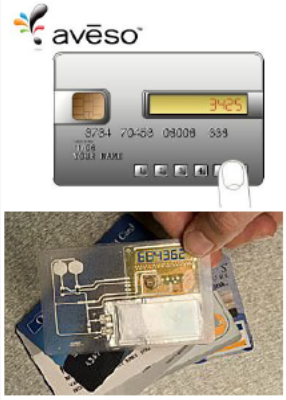

- VCC – napajanje
- GND – masa
- RST – reset
- CLK – signal takta
- I/O – ulaz/izlaz
- VPP – prog. napon
- RFU - rezervirano

**Slika 4.2.3** Izgled i značenje pojedinog kontaka

Za razmjenu podataka sa okuženjem kontaktne pametne karice posjeduju izvedene kontakte na svojoj površini. Izgled i značenje pojedinog kontakta dati su na slici

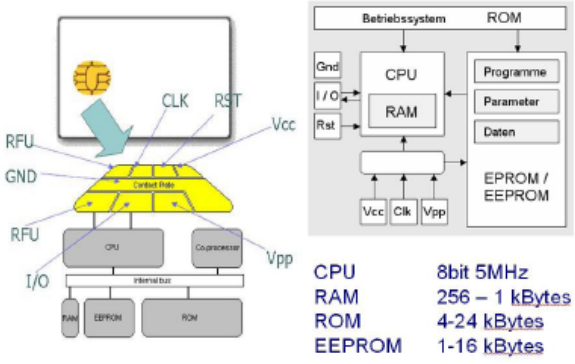
- Bezkontaktna pametna kartice, za razmjenu podataka sa okuženjem koristi antenu ugrađenu u tijelo kartice
- Hibridna pametna kartica sadrži dva čipa. Razmjena podataka sa jednim čipom vrši se preko izvedenih kontakata a sa drugim pomoću antene
- Kartice sa dvojnim interfejsom posjeduju jedan čip kome se može pristupiti i kontaktno i bezkontaktno
- Posebnu vrstu pametnih kartica predstavljaju kartica sa ugrađenim displejem i tasterima


**Slike 4.2.2** Interfejsi za razmjenu podataka sa okruženjem kod pametnih kartica




U odnosu na uobičajene, kartica sa displejem i tasterima pruža viši nivo sigurnosti identifikacije. To se ogleda u mogućnosti primjene OTP (One Time Password) koncepta, odnosno dinamičkog PIN koda. Drugim riječima, za svaki pristup sistemu upotrebljava se drugačiji PIN kod.
Statički PIN kod se unosi tasterima na samoj kartici a na displeju se dobija dinamički PIN kod za pristup sistemu. Osim toga, postojanje LCD dipleja omogućava jednostavnu provjeru stanja računa korisnika.

**4.2.4** Pametna kartica sa displejem i tastaturom




**Slika 4.2.7** Osnovni sastavni djelovi tipične mikroprocesorske kartice.

- Kao što se sa slike uočava mikroprocesorska kartica predstavlja PC u malom. Sadrži:
  - procesor (CPU) pomoću kog se vrši izračunavanje,
  - ROM (Read-Only Memory), memorija na kojoj se nalazi operativni sistem i aplikativni program,
  - RAM (Random Access Memory) memorija koja se koristi za privremeno skladištenje podataka tokom rada procesora,
  - EEPROM (Electronically Erasable and Programmable Read-Only Memory), memorija u kojoj su smješteni podaci od interesa (broj tekućeg računa, sertifikati, ključevi i sl.),
  - Takt i ulazno izlazni sklop preko koga se komunicira sa okolinom (čitačem).
- Tipična smart kartica ima 8-bitni procesor koji radi na 5MHz, 256 do 1024 KB RAM-a, 6 do 24 KB ROM-a, 1 do 16 KB EEPROM-a.
- Mikroprocesorska kartica posjeduje vlastiti operacioni sistem. Najčešće je to: Java Card, MultOS, OSCCA ili Smartcard.NET]. Omogućavaju pisanje vlastitih aplikacija koje se izvršavaju u sigurnom okruženju.
- Specijalno su konstruisane za ispunjavanje visokih sigurnosnih standarda. Visok stepen sigurnosti postiže se ugrađivanjem procesora koji obavlja enkripciju/dekripciju podataka. Povjerljivi podaci nikada nenapuštaju karticu

## SMART KARTICA
## Ka budućnosti

- Ujutro ćemo odlaziti od kuće a da nećemo morati sa sobom nositi svežanj ključeva, niti ćemo brinuti o tome da li će vrata ostati zaključana ili ne,
- Kupovina u trgovini će se obavljati bez zastoja na kasi,
- Odlazak na posao gradskim prevozom ne bi više iziskivao potrebu za sitnim novcem, žetonima ili traženjem po džepovima mesečne karte,
- Vozači automobila će bezbjedno sjedati u svoje automobile koji će se odmah pri «osećaju» svog vlasnika samostalno otključao i po mogućnosti i upalio,
- Na putevima nećemo imati problema sa drumarinom, ni sa parkiranjem ili plaćanjem goriva,

## SMART KARTICA
## Ka budućnosti

- Pozajmljivanje knjiga i kopiranje u biblioteci bi teklo bez administrativnih prepreka i obračunavanja troškova.
- Pristup Internetu, pošti i ličnim zbirkama podataka mogli bi obaviti na računarima koji će biti postavljeni duž auto-puteva bez unošenja šifri,
- Moći će se vršiti kupovina i prodaja deonica,
- Prilikom plaćanja računa u restoranima neće biti potrebe za novčanicima,
- Na kraju dana vrata od kuće bi nam se otvarala sama, upaliće se svijetla kao i stereo sa muzikom, koju smo željeli na putu do kuće,
- Odlazićemo u bioskop ili pozorište bez ulaznice.

**RAZLOZI BANAKA ZA PRELAZAK NA SMART KARTICE**

Prelazak na smart kartice za banku nije opcija nego zahtjev koji je nametnut od strane Visa i MasterCard-a. Radi regulisanja ove oblasti na globalnom nivou, Visa i MasterCard su udruženim snagama donijeli skup standarda EMV (Europay, MasterCard, Visa) koji definišu komunikaciju između smart kartice i smart card čitača. Ovaj skup specifikacija odnosi se isključivo na kreditno/debitne transakcije. Da bi banke i druge učesnike u procesu obrade transakcija sa platnim karticama primorale na migraciju, Visa (slično je i kod MasterCard-a) je propisala sledeće rokove

**Od januara 2001. godine**:

Svi novo instalirani uređaji za prihvat smart kartica moraju biti EMV/VIS (VIS=Visa International Integrated Circuit Card Specifications) saglasni,

Treba obezbediti podrška za off line PIN

Svi novi ATM uređaju pored čitača sa magnetnom trako moraju imati i čip čitač sa EMV Level 1 (hardverskim) sertifikatom

**Do oktobra 2002. godine:**

EMV terminali kod visoko rizičnih trgovaca

Acquirer-i moraju nadograditi svoje sisteme kako bi omogućili obradu EMV čip podataka

**Od oktobra 2002. godine:**

Svi novi terminali moraju biti EMV saglasni i moraju podržavati off line PIN

Postojeći čip card terminali – POS i ATM – moraju biti EMV/VIS usaglašeni.

**Od 1. januara 2006. godine:**

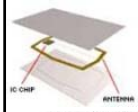
**ze CEMEA region (1. januara 2005. godine za EU)**

Ukoliko neko od učesnika u procesu (Izdavaoci) do propisanog roka nije prešao na smart tehnologiju biće odgovoran za eventualne zloupotrebe koje bi se mogle sprečiti da je nova tehnologija bila implementirana.

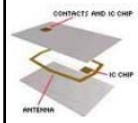
– ***Smanjenje zloupotreba***

U EMV okruženju sigurnost je jedna od najbitnijih karakteristika i prednosti. Kartica koja u sebi sadrži mikroprocesor sa sigurnosnim mehanizmima je ekstremno teška za falsifikovanje i druge načine zloupotrebe. Provjere vjerodostojnosti i autentičnosti kartica i korisnika kartica putem digitalnih sertifikata, privatnih ključeva, off line PIN-a, SDA (Static Data Authentication) i DDA (Dinamic Data Authentication) tehnika predstavlja trenutno optimalan (ako se gleda praktičnost i odnos cijena / performanse) način bezgotovinskog načina plaćanja

Kontaktna smart kartica



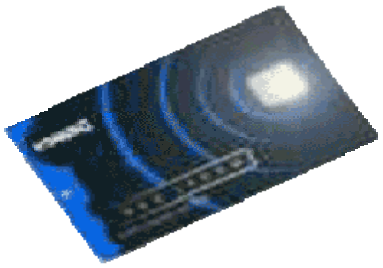

Beskontaktna smart kartica (npr. Legic ili Mifare kartica)




Hibridna, dvostruka (dva ili više ugrađenih čipova) ili kombinirana smart kartica (jedan čip kojem se pristupa putem kontakata i beskontaktno)

Ukoliko ste se prijavili za uslugu Internet bankarstva, svaku ćete transakciju, za koju ste nekada satima čekali u redu, moći obaviti s bilo kojeg računara spojenog na Internet. No, prije obavljanja bilo koje transakcije, morаćete se autorizovati. Postoji nekoliko načina autorizacije. Za privatne korisnike su to najčešće **tokeni** ili **TAN-ovi**, dok pravne osobe u pravilu koriste ***smart*-kartice**. Zavisno o banci i tehnološkoj pozadini, nudi Vam se jedna od pomenutih načina autorizacije. Ponekad banke nude i izbor između dvije različite metode. Visokim stepenom sigurnosti ističe se autorizacija putem *smart*-kartica, dok je autorizacija pomoću tokena prihvatljiva u pogledu i cijene i sigurnosti. Metoda autentifikacije pomoću TAN-ova sve je manje i manje u upotrebi.

*Smart*-kartica je kartica u kojoj se nalazi ili mikroprocesor i memorijski čip ili samo memorijski čip s neprogramabilnom logikom. Na kartici koja sadrži mikroprocesor postoji mogućnost upisivanja podataka, brisanja ili neke druge vrste manipulacije podacima. Kartica koja ima samo memorijski čip može izvoditi samo predefinisane funkcije. *Smart*-kartice, za razliku od kartica sa magnetskom trakom, sadrže sve potrebne funkcije i informacije potrebne za Vašu autorizaciju, zbog čega u trenutku transakcije nije potreban pristup udaljenim bazama podataka



**Kako biste ih mogli koristiti, na računaru morate imati instaliran čitač *smart*-kartica**. Čitač, kao i softver potreban za instalaciju čitača na računaru, korisnik mora kupiti od banke pri registraciji za uslugu.

Kartica se temelji na PKI (*Public Key Infrastructure*) tehnologiji koja se zasniva na asimetričnoj kriptografiji, odnosno na paru **javnih** i **tajnih ključeva** za šifriranje podataka. Svaki korisnik ima svoj tajni ključ i svoj javni ključ. Samo je javni ključ korisnika dat drugima na uvid. Korisnik podatke koje želi nekome poslati šifrira svojim tajnim ključem. Kada bi se takvi podaci poslali, pročitati bi ih mogao svako ko posjeduje javni ključ pošiljatelja. Iz tog razloga pošiljatelj šifrira podatke još jedanput, ovaj put javnim ključem primatelja podataka. Na taj su način podaci dostupni samo primatelju. Naime, primatelj ih mora dešifrirati najprije pošiljateljevim javnim ključem, a zatim i svojim tajnim ključem. Svi su ti ključevi u digitalnom obliku pohranjeni na *smart*-kartici.

*Smart*-kartica se uveliko razlikuje od kreditne kartice uprkos sličnostima u obliku i veličini.

Dok je u unutrašnjost *smart*-kartice umetnut 8-bitni mikroprocesor, normalna kreditna kartica u potpunost je sačinjena od plastike. Mikroprocesor se u *smart*-kartici nalazi ispod zlatnog čipa na prednjoj strani kartice. Na čip se može gledati kao na zamjenu za magnetsku traku prisutnu na kreditnim ili debitnim karticama.

Kod magnetskih traka podaci se mogu jednostavno čitati, upisivati, brisati ili pak mijenjati. Kako pristup podacima ne bi bio tako jednostavan, na *smart*-kartice se ugrađuje mikroprocesor.

Najčešće primjene *smart*-kartica su:

- •kreditne kartice
- •elektronske kartice
- • za Internet bankarstvo
- •kod kodiranih satelitskih programa
- •kao identifikacije u vladinim institucijama
- •kod bežične komunikacije
- •kod računarskihih sigurnosnih sistema
- •kod mobilnih uređaja na karticu

## Token

- Kod korišćenja usluga Internet bankarstva kao najbolja metoda autorizacije ističe se **token**, koji predstavlja kompromis između cijene i učinka.
- Korišćenje tokena smanjuje rizik od neovlašćenog pristupa podacima, a ne zahtijeva nikakva finansijska ulaganja od strane korisnika.
- Token je uređaj nalik džepnom kalkulatoru.
- Jedan se takav uređaj ustupa klijentu na privremeno korišćenje prilikom registracije za uslugu Internet bankarstva. Prilikom odjave usluge klijent je dužan vratiti uređaj u filijalu u kojoj ga je primio.

- Numeričke tipke na tokenu omogućavaju korisniku unos **PIN-a** (Personal Identification Number) koji je nužan za uspješnu autorizaciju kod samog tokena.
- PIN je broj od četiri do osam cifara kojeg korisniku ustupa banka. Nakon prve autorizacije korisnik ima mogućnost promijeniti PIN za otključavanje uređaja.
- Nakon autorizacije token generiše niz brojeva koji se zajedno sa serijskim brojem tokena mora unijeti u aplikaciju.
- Serijski broj svakog tokena je jedinstven i sačinjava dio kriptografskog ključa koji omogućuje generisanje dinamičkog koda za pristup mreži. Da bi se spriječilo presretanje podataka u mreži, postoje i drugi načini zaštite kao što je zaštita putanje kojom se vrši protok podataka.

• Pri autorizaciji i validaciji podataka poslužitelj, u banci, generiše ***challenge***, odnosno numeričku vrijednost sačinjenu od šest cifara. Te se cifre dobiju iz datuma, vremena izvođenja transakcije i same novčane vrijednosti transakcije.

• Da bi se uspješno provela transakcija, klijent mora utipkati *challenge* u token koji nakon toga generiše ***challenge response***. *Challenge response* se također sastoji od šest cifara i valjan je samo za izvođenje trenutne transakcije.

• Poslužitelj na temelju *challenge* niza izračunava ispravni *challenge response* niz i uspoređuje ga s nizom kojeg unosi korisnik kako bi potvrdio integritet transakcije. Broj koji token generše za jednokratnu je upotrebu, odnosno ne postoji mogućnost ponavljanja generisanog niza. Klijent ima na raspolaganju određeni vremenski period u kojem mora unijeti generisani niz. Taj period traje od 30 do 60 sekundi nakon čega se token automatski isključuje

- Ovakav model autorizacije koji se sastoji od dva faktora (serijskog broja tokena i niza brojeva koje token generiše) omogućava računaru u banci da jednoznačno identifikuje klijenta te mu omogući pristup svim njegovim računima.
- Dakle, sigurnosni mehanizam ugrađen u token je usklađen s poslužiteljem koji provjerava parametre autorizacije. Ukoliko klijent unese neispravan PIN nekoliko puta za redom, na primjer tri puta, token se automatski zaključa.
- Administrator je jedina autorizirana osoba za otključavanje uređaja. Ukoliko se pak unese neispravan kod za autorizaciju korisnika, web aplikacija se terminira. Svaki se takav pokušaj zabilježi kod poslužitelja.
- Administrator pregleda zabilješke i na taj način može uočiti sumnjive radnje pri autorizaciji.

- Prednost **tokena** pred TAN-ovima je jednostavna administracija. Nakon što jednom ustupi token klijentu na korišćenje, banka se ne mora brinuti oko njegove dalje autorizacije, kao što je to u slučaju TAN-ova. Nedostatak tokena je to što klijent mora uređaj nositi sa sobom ukoliko želi obaviti neku bankarsku transakciju na različitim mjestima. Uz navedeno tu je još i velika i nepregledna količina brojeva koja se mora unijeti u web-aplikaciju.

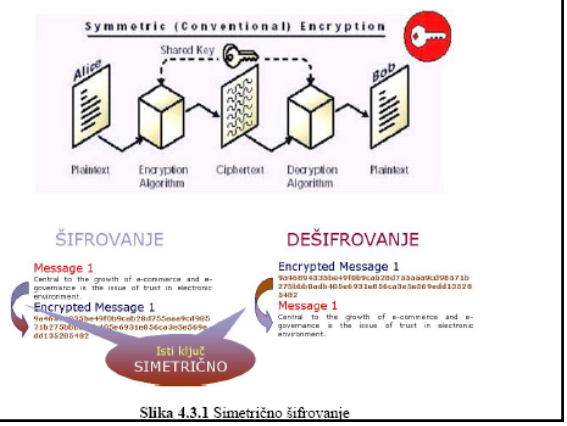
## TAN

- Autorizacija putem TAN-ova obično podrazumijeva list papira s pedesetak ili stotinjak nizova cifara koje klijent prima od banke. Kada klijent iskoristi sve nizove s liste, banka mu poštom šalje novu listu.
- Pojedine banke, pak, izdaju karticu s određenim brojem TAN-ova koje tada korisnik kružno koristi pri čemu nema potrebe za primanjem novih TAN-ova.
- TAN-ovi izgledaju poput telefonskih brojeva pa je time smanjena opasnost zloupotrebe u slučaju krađe ili provale. Velika prednost ove metode autorizacije jest to što ne zahtijeva nošenje uređaja za obavljanje bankarskih transakcija. Korisnik može sa sobom uvijek imati nekoliko TAN-ova u slučaju potrebe za obavljanjem neke transakcije. S druge strane veliki nedostatak TAN-ova čini teška administracija.

- Naime, banka mora čuvati u svojoj bazi popis TAN-ova za svakog klijenta, kako potrošenih, tako i tek dodijeljenih TAN-ova.

# KRIPTOVANJE PODATAKA

- U cilju zaštite podataka, u komunikaciji sa pametnim karticama koriste se sljedeći algoritmi kriptovanja:
  - Simetrični algoritmi kriptovanja,
  - Asimetrični algoritmi kriptovanja i digitalni potpis
- Simetrični algoritmi kriptovanja za kriptovanje i za dekriptovanje upotrebljavaju jednostavno povezane, često identične, kriptografske ključeve. Ključevi su ili identični ili se jednostavnom transformacijom iz jednog izvodi drugi ključ. U ovom načinu šifrovanja ključevi predstavljaju dijeljenu tajnu između dvije ili više strana

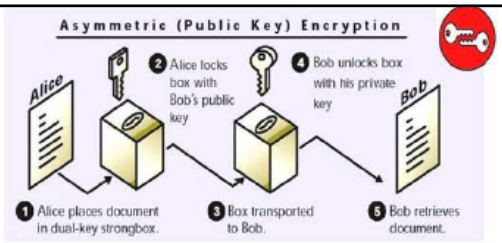



Slika 4.3.1 Simetrično šifrovanje

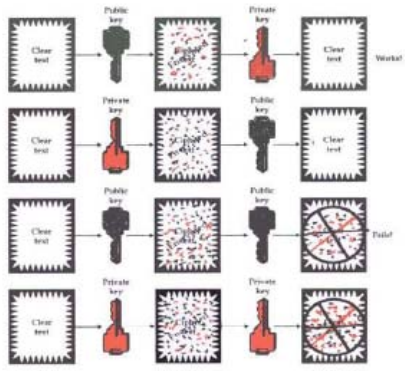
- Drugi nazivi za simetrično šifrovanje su sifrovanje sa tajnim-ključem (secret-key), jedinim-ključem (single-key, one-key), dijeljenim-ključem (sharedkey), ili, eventualno, privatnim-ključem (privatekey).
- Posljednji naziv ne preba miješati sa terminom privatni-ključ u asimetričnim algoritmima šifrovanja.
- Algoritmi simetričnog šifrovanja se mogu podijeliti u dvije grupe i to:
  - *stream ciphers* i
  - *block ciphers* algoritmi.
- *Stream ciphers* algoritmi kodiraju bit po bit poruke, dok *block ciphers* algoritmi uzimaju blok bitova poruke i šifruju ga kao jednu cjelinu.
- *Block ciphers* algoritmi najčešće uzimaju po 64 bita. *Advanced Encryption Standard* algoritam, prihvaćen od *NIST*-a (National Institute of Standards and Technology) u Decembru 2001 godine ima 128 bitova u jednom bloku.
- Neki od popularnih simetričnih algoritama šifrovanja su: *Twofish*, *Serpent*, *AES* (ili Rijndael), *Blowfish*, *CAST5*, *RC4*, DES, *TDES*, and *IDEA*

## ASIMETRIČNA KRIPTOGRAFIJA

- Asimetrično kriptografija, takođe poznata i kao kriptografija javnim ključem, je vrsta kriptovanja u kojem se ključ za šifrovanje podataka razlikuje od ključa za dešifrovanje.
- Svaki korisnih upotrebljava par ključeva poznatih kao javni i privatni ključ. Privatni ključ se čuva u tajnosti dok je javni ključ poznat svima zainteresovanima.
- Važno je naglasiti da se poznavanjem javnog ključa ne može izračunati tajni ključ u nekom razumnom vremenu




- Pristigla poruka, koja je šifrovana primaočevim javnim ključem može biti dešifrovana samo njegovim tajnim ključem i obrnuto (Slika 4.3.20).
- Ključevi su matematički povezani, ali se privatni ključ praktično ne može izvesti iz javnog ključa.



**Slika 4.3.20** Asimetrična kriptografija – osnovni princip

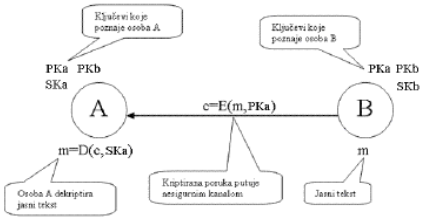
- Dvije glavne grane asimetrične kriptografije su:
  - **Šifrovanje javnim ključem** - poruka šifrovana primaočevim javnim ključem može biti dešifrovana jedino primaočevim tajnim ključem. Ovakav vid asimetričnog šifrovanja koristi se da obezbijedi povjerljivost (tajnost) poruke.
  - **Digitalni potpis** - Poruka potpisana pošiljaočevim privatnim ključem, može biti verifikovana od strane bilo koga ko poznaje pošiljaočev javni ključ. Ovakav vid asimetričnog šifrovanja koristi se da obezbijedi potvrdu autentičnosti poruke.

- Algoritmi asimetrične kriptografije mogu se svrstati u tri osnovne grupe:

  1. algoritmi zasnovani na praktičnoj nemogućnosti faktoriziranja velikih prostih brojeva (RSA),

  2. algoritmi zasnovani na praktičnoj nemogućnosti izračunavanja diskretnih logaritama (Diffie-Hellman protokol, DSA)

  3. algoritmi zasnovani na eliptičnim krivuljamama (praktične realizacije ove metode su tek u povojima)




**Slika 4.3.21** Šema rada asimetričnog kriptografskog sistema.

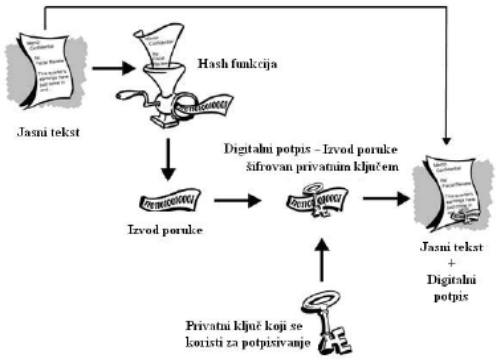
Glavni cilj ovoga načina kriptovanja je da pruži privatnost i pouzdanost. Međutim, pošto je javni ključ osobe A svima poznat, ovakav kriptografski sistem ne osigurava da se pouzdano zna odakle (od koga) je poruka stigla, a ne može se sa sigurnošću potvrditi niti integritet podataka. Da bi se obezbijedila autentičnost pošiljatelja potrebno je da poruka bude kodirana ili potpisana i privatnim ključem pošiljatelja

- Asimetrični algoritmi daleko su sporiji od simetričnih algoritama kao npr. DES. Upravo zbog tog razloga kriptovanje asimetričnim algoritmima najčešće se koristi za:
  - Izmjenu ključeva za poruke koje su kriptovane simetričnim algoritmima
  -Zaštitu malih blokova podataka (primjer : PIN-ovi na pametnim karticama)
- Najčešće korišteni algoritam asimetrične kriptografije je RSA algoritam, koji pripada prvoj grupi algoritama asimetrične kriptografije.
- Dužina ključeva za algoritam RSA uobičajeno je 1024 bita. Kriptovanje sa 512 bitova više se ne smatra sigurnim. Za potpunu sigurnost preporučuje se 2048 odnosno 4096 bitova.

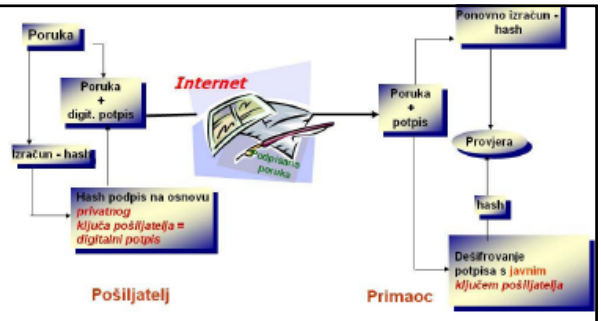
## Digitalni potpis

- Digitalni potpis je oblik asimetrične kriptografije koji se koristi kao zamjena za svojeručni potpis. Digitalni potpis obezbjeđuje autentičnost "poruke". Poruka može biti bilo što, od elektronskog pisma do ugovora.
- Šema digitalnog potpisa se sastoji od tri algoriutma:
  1. Algoritam za generisanje ključa – selektuje privatni ključ iz seta mogućih privatnih ključeva. Kao rezultat, ovaj algoritam vraća privatni i odgovarajući javni ključ.
  2. Algoritam potpisivanja – iz date poruke i privatnog ključa generiše digitalni potpis.
  3. Algoritam za verifikaciju potpisa – na osnovu potpisane poruke i javnog ključa obavlja verifikaciju digitalnog potpisa.

- Digitalni potpis mora zadovoljiti dva osnovna zahtjeva:
- Prvi, potpis generisan iz fikne poruke i fiksnog privatnog ključa može se verifikovati jedino na toj poruci sa odgovarajućim javnim ključem.
- Drugi, treba biti računski neizvodljivo generisati validan potpis, od strane onog ko ne posjeduje privatni ključ.

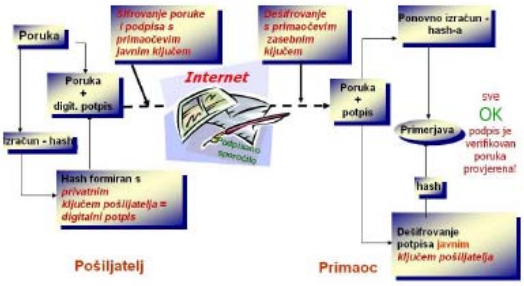



**Slika 4.3.24** Postupak potpisivanja poruke digitalnim potpisom




**Slika 4.3.25** Ilustrativni prikaz postupka slanja i prijema poruke sa digitalnim potpisom

- Osim autentičnosti primaoc može biti siguran i u integritet podataka u poruci. Ovo proističe iz toga što je izvod zavistan od sadržaja poruke.
- Svaka, i najmanja, izmjena poruke reflektuje se na vrijednoist izvoda.
- Prema tome, ukoliko bi poruka, od trenutka slanja do trenutka prijema, bila izmijenjena od stane trećeg lica izračunati i dešifrovani izvod se ne bi podudarili. Iz ovog proističe da je digitalni potpis različit od poruke do poruke i obezbjeđuje autentičnost svake riječi u dokumentu.




Slika 4.3.27 Ilustativni prikaz postupka slanja i prijema šifrovane poruke sa digitalnim potpisom

| Parametar | Papir | Electronika |
|---|---|---|
| Autentičnost | Može se krivotvoriti | Ne može se kopirati |
| Integritet | Potpis nezavistan od dokumenta | Potpis zavisi od sadržine dokumenta |
| Prihvatanje-odbacivanja | a. Potreban ekspert za rukopise<br>b. Moguća greška | a. Svaki kompjuter<br>b. Bez greške |

Tabela 4.3.8 Poređenje osobina ručnog i digitalnog potpisa

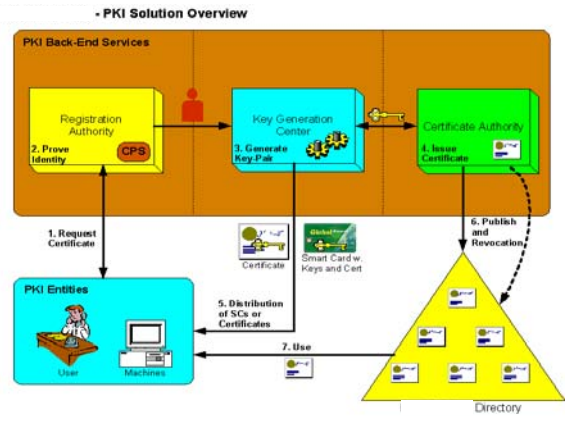
## Žaštita privatnog ključa

•Kao što je već rečeno privatni ključ se mora čuvati u tajnosti. Najčešći načini čuvanja su:
- Na hard disku računara.
- Unutar pametne kartice.
- Unutar hardverskog modula (iKey)

Slika 4.3.28 Uređaji koji se koriste za čuvanje privatnog ključa

- Na hard disku računara šifrovani ključ se čuva u fajlu koji je zaštićen lozinkom. Ovo se smatra najnesigurnijim načinom čuvanja privatnog ključa. Ovo stoga što samim tim što se nalazi na hard diku, ključ dostupan a lozinka se može saznati ili razbiti.
- Ukoliko se privatni ključ čuva u pametnoj kartici to podrazumijeva da se on generiše u kripto modulu kartice i ostaje u kartici. Ključ se čuva u memoriji kartice i veoma je bezbjedan jer je nikad ne napušta. Izvod poruke se šalje kartici na potis i potpis napušta karticu. Kartica obezbjeđuje prenosivost ključu, pa se potpisivanje može vršiti bilo gdje, gdje postoji čitač kartica.
- Čuvanjem privatnog ključa unutar hardverskog modula (iKey-a) postiže se funkcionalnost i zaštita slična pametnoj kartici. Kao prednost iKey-a može se navesti to on ne zahtijeva specijalni čitač već se može priključiti na USB port računara.

# Infrastruktura javnih ključeva PKI



## PKI pozadinski servisi

- PKI pozadinski servisi mogu se grubo podeliti u tri cjeline:
  - · Registraciona tijela (RA)
  - · Generisanje ključeva (KG)
  - · Sertifikaciono telo (CA)

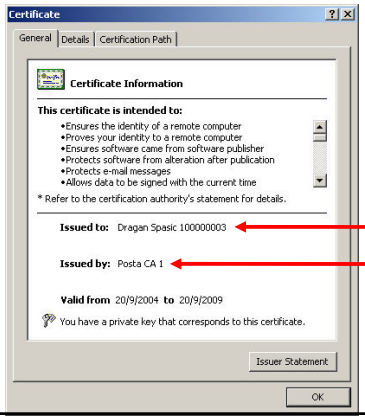
## Sertifikaciono tijelo
## CA "certifying authority"


## Uvod - Digitalni identitet (Digital ID)


## Uvod - Digitalni identitet (Digital ID)

- Digitalni identitet korisnika čine:
  1. tajni (privatni) kriptografski ključ (private key) korisnika,
  2. javni kriptografski ključ (public key) korisnika i
  3. digitalni sertifikat (digital certificate) koji sadrži javni kriptografski ključ korisnika.
- Digitalne sertifikate korisnicima izdaju sertifikaciona tela (Certification Authority - CA).
- Sertifikaciona tela poseduju PKI infrastrukturu (Public Key Infrastructure - PKI).

## Pojam digitalnog (elektronskog) sertifikata




Ime korisnika

Ime sertifikacionog tela (CA servera)

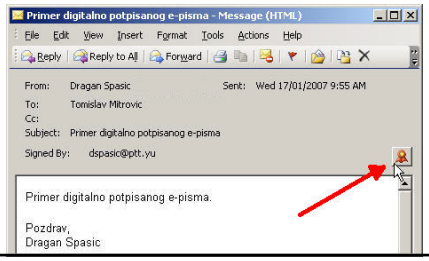
Javni ključ korisnika

## Mediji za digitalne sertifikate

- Hard disk, disketa ili CD,
- PKI smart kartica,
- PKI USB smart token.

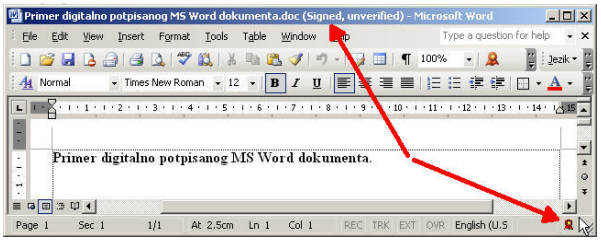
## Pojam digitalnog (elektronskog) potpisa

- Digitalni potpis nije skenirani svojeručni potpis.
- Digitalni potpis omogućava: autentifikaciju tj. identitet potpisnika, integritet el. dokumenta i neporecivost.
- Primer digitalno potpisanog e-pisma:




## Pojam digitalnog (elektronskog) potpisa

- **Primer digitalno potpisanog Microsoft Word**




- I druge aplikacije omogućavaju digitalno potpisivanje.

## Sertifikaciono telo (Certification Authority - CA)

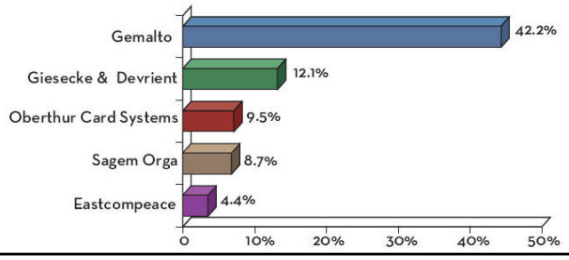
- Sertifikaciono tijelo je pravno lice koje izaje digitalne (elektronske) sertifikate korisnicima.

- Sertifikaciona i registraciona tela su po pravilu komercijane institucije, a u mnogim državama su **Pošte** sert. tela:

1. Post.Trust (http://www.post.trust.ie), Pošta Irske (http://www.anpost.ie).
2. Postecom (http://www.postecom.it), Pošta Italije (http://www.poste.it).
3. Signtrust (http://www.signtrust.de), Pošta Nemačke (http://www.deutschepost.de).
4. Certinomis (http://www.certinomis.com), Pošta Francuske (http://www.laposte.fr).
5. Certipost (http://www.certipost.be), Pošta Belgije (http://www.post.be).
6. Multicert (http://www.multicert.pt), Pošta Portugalije (http://www.ctt.pt).
7. Buypass (http://www.buypass.no), Pošta Norveške (http://www.posten.no).
8. Post Signum (http://www.postsignum.cz), Pošta Češke (http://www.cpost.cz).
9. E-paraksts (http://www.e-me.lv), Pošta Letonije (http://www.pasts.lv).
10. Certifikatska agencija Pošte Slovenije (http://postarca.posta.si), Pošta Slovenije (http://www.posta.si).
11. KeyPOST (http://www.auspost.com.au/keypost), Pošta Australije (http://www.auspost.com.au).
12. Hongkong Post e-Cert (http://www.hongkongpost.gov.hk), Pošta Honkonga (http://www.hongkongpost.com).

## Francuska i Njemačka

- Francuska (62 miliona stanovnika) i Njemačka (83 miliona stanovnika) su vodeće države u svijetu u oblasti tehnologije smart kartica. Prva 4 proizvođača smart kartica su Francuske i Njemačke kompanije, i imale su udio na svetskom tržištu od **72,5%** tokom 2005. godine:




## Sertifikaciona tijela u Francuskoj

- Na Web strani koju održava francusko Ministarstvo ekonomije, finansija i industrije, postoji spisak sertifikacionih tijela (http://www.telecom.gouv.fr):


## Sertifikaciona tela u Njemačkoj

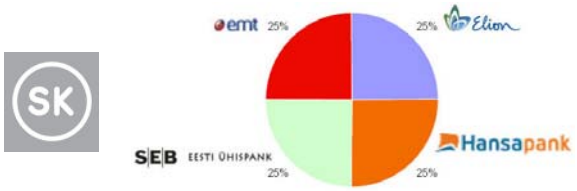
- 28 registrovanih sertifikacionih tijela za izdavanje kvalifikovanih sertifikata, navedeno je na Web strani koju održava nemačka Federalna agencija za električnu energiju, gas, telekomunikacije, poštu i železnicu (http://www.nrca-ds.de):

## Sertifikaciono tijelo u Belgiji

- U Belgiji (10,5 miliona stanovnika) građani dobijaju sertifikate na e-ličnim kartama, koje su obavezne.
- Sertifikate izdaje kompanija **Certipost** (http://www.certipost.be), koju su formirali Pošta Belgije (Belgian Post Group - BPG) i kompanija Belgacom:


## Sertifikaciono telo u Estoniji

- U Estoniji (1,5 miliona stanovnika) građani dobijaju sertifikate na e-ličnim kartama, koje su obavezne.
- Sertifikate izdaje kompanija SK Certification Centre (http://www.sk.ee), koju su formirali dve vodeće banke u Estoniji i dve telekomunikacione kompanije:




## Sertifikaciona tijela u Sloveniji

- U Sloveniji (2 miliona stanovnika) postoje četiri (4) registrovana sertifikaciona tijela za izdavanje kvalifikovanih digitalnih sertifikata:

1. Ministarstvo za javnu upravu, koje ima dva CA servera: SIGEN-CA (http://www.sigen-ca.si) koji izdaje sertifikate fizičkim i pravnim licima, i SIGOV-CA (http://www.sigov-ca.gov.si) koji izdaje sertifikate zaposlenima u javnoj upravi.
2. HALCOM informatika d.o.o., Služba HALCOM-CA, http://www.halcom.si.
3. Nova Ljubljanska banka d.d., AC (Agencija za sertifikovanje) NLB, http://www.nlb.si/acnlb.
4. Pošta Slovenije d.o.o., POŠTA CA, http://postarca.posta.si.

- Primer e-Government-a: Prijava poreza (eDavki

## Sertifikaciona tijela u Austriji

- U Austriji (8,2 miliona stanovnika) ne postoji samo jedna elektronska identifikaciona kartica građana, već više različitih kartica koje izdaju različite institucije:

1. Kartice koje izdaju sertifikaciona tela. U ovom trenutku ovlašćeno je samo jedno sertifikaciono telo, koje je jedino sertifikaciono telo koje izdaje kvalifikovane sertifikate: A-Trust, http://www.a-trust.at.
2. Kartice zdravstvenog osiguranja "e-card" (http://www.chipkarte.at).
3. Bankarske kartice.
4. Identifikacione kartice Federalnih ministarstava.
5. Kartice koje izdaju različite komore i udruženja (na primer: Privredna komora, Javni beležnik-notar, Austrijsko kompjutersko udruženje,...).
6. Studentske kartice.
7. SIM kartice mobilne telefonije koje izdaje operater mobilne telefonije A1 (http://www.a1.net/privat/a1signatur), tj. Mobilkom Austria AG.

- Za navedene kartice sertifikate izdaju sledeća sert. tijela:

1. Kompanija A-Trust.
2. Kompanija A1, tj. Mobilkom Austria AG.
3. Glavno udruženje institucija za socijalnu zaštitu (za "e-card" kartice).

## Austrija: sertifikati na SIM karticama

- U Austriji za e-Government mogu da se koriste sertifikati na SIM karticama mobilne telefonije (na primer: https://www.zustellung.gv.at ili https://meldung.cio.gv.at/egovMB):


## Sertifikaciono tijelo u Finskoj

- U Finskoj (5,3 miliona stanovnika) sertifikati građana mogu da se uskladište i koriste i sa sledećih kartica:

1. E-lične karte, koje nisu obavezne za građane (http://www.fineid.fi).
2. Visa Electron kartice koje izdaje OP banka (https://www.op.fi).
3. SIM kartice mobilne telefonije koje izdaju operateri mobilne telefonije: Sonera (http://www.sonera.fi) i Elisa (http://www.elisa.fi).

- Za navedene kartice sertifikate izdaje **Centar za registrovanje građana** (Population Register Centre - PRC, http://www.vaestorekisterikeskus.fi), koji je trenutno jedino sertifikaciono tijelo u Finskoj koje izdaje kvalifikovane sertifikate.

## Zaključak

- Za potrebe e-Government-a tj. e-Uprave u Crnoj Gori, građanima treba izdati (dodeliti) digitalne sertifikate. Pri tome:
- Izdavanje digitalnih sertifikata građanima treba da bude na dobrovoljnoj osnovi.
- Građanima treba dati mogućnost da samostalno izaberu od kog će sertifikacionog tijela da nabave tj. kupe digitalne sertifikate.
- Građanima treba dati mogućnost da samostalno izaberu medijum na kome će biti uskladišen njihov digitalni sertifikat i tajni ključ (hard disk, smart kartica, USB smart token, SIM kartica,...).
- E-lične karte sa čipom nijesu neophodne za uvođenje e-Government-a.

## Registraciona tijela (RA)

- Osnovni zadatak Registracionih tijela (RA) je da provjere identitet osobe koja zahtijeva sertifikat.
- To je organizacioni proces koji treba da je definisan i uspostavljen od CeP prije nego što se izdaju prvi sertifikati.
- Svi RA slede propisanu politiku izdavanja sertifikata.
- Na primjer, registracija za privatna lica zahtijeva od osobe da prezentuje fotografiju.
- Politika izdavanja sertifikata je definisana u Povelji o sertifikaciji (Certification Practice Statement - CPS). CPS je javno objavljen dokument koji uspostavlja legalnu infrastrukturu i operacione procedure za Sertifikaciono telo (CA).

## Generisanje ključeva (KG)

- Key Generation (KG) stupa na scenu nakon što je dokazan identitet zahtjevaoca sertifikata.
- Par ključeva (privatni i javni) se generiše ili centralizovano ili interno unutar određenih komponenata (smart kartice) u zavisnosti od zahtjevaoca.
- Javni ključ se šalje CA radi izdavanja sertifikata.
- Privatni ključ se arhivira za potrebe eventualnog oporavka (gubitka i sl.) i to samo u slučajevima kada je politikom izdavanja sertifikata predviđeno čuvanje tajnog ključa.
- Smart kartica može sadržavati više od jednog para ključeva, kao što su par ključeva za digitalno potpisivanje i drugi par za šifrovanje i autentifikaciju.
- Dodatno, smart kartice se personalizuju uz definisanje tzv. ličnog identifikacionog broja (personal identification number - PIN).

## Sertifikaciono telo (CA)

- CA izdaje ili obnavlja sertifikate koji su, ili za korisnika, ili za određenu aplikaciju.
- Sertifikat je dokument koji je digitalno potpisan od strane CA i koji povezuje određeni entitet sa određenim javnim ključem.
- Ostale funkcije CA uključuju operacije :
  - arhiviranja i oporavka
  - publikovanje
  - povlačenje sertifikata.

## Trajanja važnosti sertifikata (validity period)

- Što je duže u upotrebi javni i privatni ključ, više paketa će biti zaštićeno istim parom ključeva, dajući hakerima više vremena da razbiju matematički problem koji leži u osnovi asimetričnih šifara. Međutim, dobra je praksa da se zanovi par ključeva svaki put kada se zanavlja sertifikat.
- Trajanje sertifikata je zavisno i od dužine ključa. Zato što je potrebno manje vremena za rješavanje matematičkog problema za šifrate u kojima je korišćen kraći ključ, sertifikati koji sadrže kraći javni ključ treba da imaju kraći životni ciklus od sertifikata koji sadrže duži javni ključ.

## Trajanja važnosti sertifikata (validity period)

- Smještaj sertifikata (time i javnog ključa) na posebne medije (kao što su smart kartice), i korišćenje hardverskih CSP, smanjuje rizik kompromitacije privatnog ključa. To je razlog za moguće produženje životnog vijeka, kako para ključeva, tako i sertifikata.
- Sigurniji smeštaj automatski smanjuje rizik napada na javni ključ - još jedan razlog za razmatranje dužeg životnog ciklusa sertifikata.

Trajanja važnosti sertifikata (validity period)

- Ako se izdaju sertifikati korisnicima van poslovno-tehničkog sistema, životni vijek sertifikata može biti kraći nego kada se izdaju sertifikati korisnicima unutar poslovno-tehničkog sistema.
- Generalno, nivo povjerenja koji organizacija ima u svoje zaposlene je veći nego nivo povjerenja koji ima u eksterne korisnike poslovno-tehničke IT infrastrukture.

**Mjere za povećanje bezbjednosti CA servera**

- Privatni ključ CA je najkritičniji element PKI sigurnosti.
- Ako se kompromituje privatni ključ korjenskog ili međustepenog CA, dio ili cijela PKI-povjerljiva infrastruktura je ruinirana.
- Nivo zaštite koji obezbeđuje CA kod čuvanja svog privatnog ključa ima značajnog uticaja na nivo poverenja koji korisnici imaju u CA.
- To je razlog zašto je toliko važno da se privatni ključ CA čuva posebno zaštićen, i da se root i međustepeni CA drže off-line.

**Mjere za povećanje bezbjednosti CA servera**

- ·**Fizičko obezbjeđenje**. Instalirati Sertifikat servere na računare u *zaštićenom prostoru* gde je moguće kontrolisati fizički pristup i gde je obezbijeđena zaštita od požara, gubitka napajanja, i ostalih fizičkih nepogoda.
- ·**Logička zaštita**. Implementirati softversku kontrolu pristupa na svim računarima da bi se spriječio neovlašćen pristup računarskim sistemima.
- ·Može se obezbijediti autentikacija visokog kvaliteta dogradnjom servera sa čitačima smart kartica.
- Autentikacija korisnika na bazi sertifikata smeštenih na smart kartici obezbjeđuje vrlo pouzdanu autentikaciju.
- ·Može se obezbediti kontrola pristupa visokog nivoa kontrolom ACL lista nad svim serverskim resursima u regularnim vremenskim intervalima.

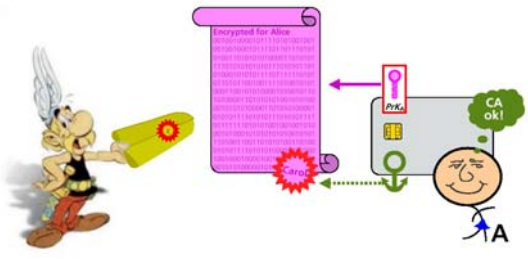
**Mjere za povećanje bezbjednosti CA servera**

- ·**Zaštita komunikacija**. Da bi se obezbijedila zaštita komunikacija za CA (CA koja izdaju sertifikate ili drugi on-line CA), a koji su konektovani na produkcijsku mrežu, CA servere treba da instalirate u posebnu podmrežu, iza namjenskog firewall-a ili rutera koji filtrira sav ne-PKI saobraćaj.
- ·**Organizacione mjere zaštite**. Morate biti sigurni da administrativno osoblje CA i operatori u računarskoj sali gde je smešten CA server, shvataju važnost CA.
- Posebno im treba naglasiti da to nije običan fajl ili print server nego server koji se koristi da zaštiti poslovno-tehničko IT okruženje.

## Budućnost PKI-ja

- U budućnosti se očekuje šira upotreba prenosnih komunikacionih uređaja, pa i elektroniskih transakcija putem njih, što je posledica povećanja broja korisnika i usluga.
- PDA uređaji, mobilni telefoni i prenosni računari, u kombinaciji s pametnim karticama, sve će se više koristiti kao bežični identifikacijski tokeni.
- Poveća će se i primjena biometrijskih metoda (skeniranje otiska prsta, glasa, lica, zenice oka...).
- Povećanjem snage računara trenutno korišćeni enkripcijski algoritmi ubrzo bi mogli zastariti, a morali bi ih zamijeniti novi, složeniji i sigurniji algoritmi.

**Digitalni POTPIS**



## TEHNOLOGIJE ELEKTRONSKOG I DIGITALNOG POTPISA

- skenirani ručni potpis
- biometrijski potpis ( Biometric Signature Verification )
- digitalni potpis (Kriptografija javnog kljuca)

## SKENIRANI RUČNI POTPIS

- digitalni ručni potpis u seriju bitova i upisan u datoteku potpisa
- provjera potpisa
- poređenje primljenog potpisa sa onim iz datoteke
- mijenjanje dokumenta nema uticaja na izgled potpisa

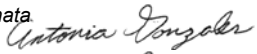
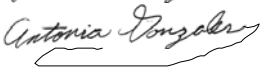
## Tabla za potpis

- Potpisnik potpisuje tablet specijalnom olovkom
- Softver koriguje pukotine u potpisu tako da ja neprekidan
- I invalidi mogu da koriste ovaj uredjaj

## Verifikacija potpisa

- *Mjerene promjenljive*
  - *–Izgled/oblik*
  - *–Brzina*
  - *–Pritisak*
  - *–Pozicije/pojave podizanja olovke*
  - *–Br linijskih segmenata*
  - *–Ukupno vrijeme*
  - *–Min, Max brzine*



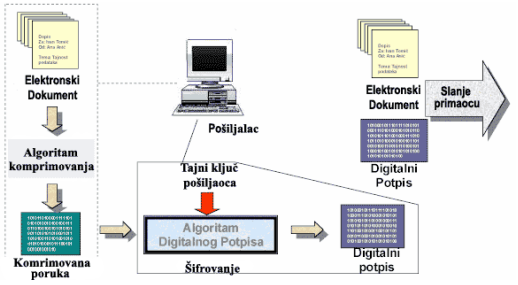



- *Ignoriše potpise*
- *Uči iz svake verifikacije*

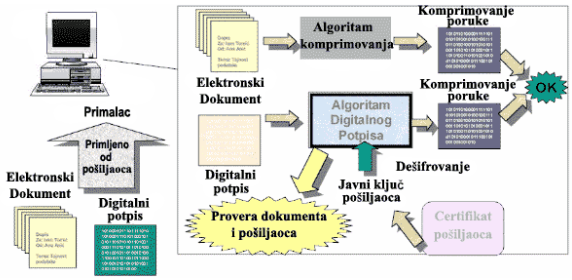
## DIGITALNI POTPIS

- identifikaciju učesnika na mreži
- provjeru cjelovitosti poslate poruke
- nemogućnost odbijanja poslatog dokumenta


## Kreiranje digitalnog potpisa



## Provjera digitalnog potpisa




## Primer dokumenta potpisanog elektronski

- **Naziv preduzeca: OSTREX-TRADE**
  **E-mail: ostrex@ptt.yu**
  **Dat.unosa: 2002-07-15**
- **Informacija: Suvlasnik sam firme koja zaposljava 5 radnika, a pored toga posedujemo i firmu u Slovackoj, koje se bave prvenstveno trgovinom, mada je u planu prosirenje na neke proizvodne delatnosti. Mi smo spremni za svaki oblik udruzivanja i/ili ulaganja u nasu firmu sa stranim investitorima**
- **--- BEGIN PGP SIGNATURE ---**
- **Version: 2.6.2**
- **owHtjukioedSftkuk+38Gtuzer+BeZgui79L03flcopertUNj@UuhX2 soUspaufVsfopS u8tby1kUXTGsFhAgsEYa 0/eed9+59917j3nsS17746789Retyiop47987HgiuopŠtrvgui0456/aj W/7rlIBrj/Zbf WrtopHGz467/opšthikkuekopBV562Rmj2nd Frt 1d8dNmyvvq12K7tj89opLxf**
- **--- END PGP SIGNATURE ---**

## POMOĆU CERTIFIKATA PRIMALAC

- - IDENTIFIKIUJE POŠILJAOCA
  - dešifrovanjem poruke javnim ključem pošiljaoca provjerom u bazi certifikata
- PROVJERA DIGITALNOG POTPISA
  - kreiranje komprimovanog dokumenta iz primljenog dokumenta
  - izrada komprimovanog dokumenta iz digitalnog potpisa
  - ako su kompresije iste, poruka nije mijenjana u prenosu

## STRUKTURA CERTIFIKATA – norma ISO X.509 Ver 3

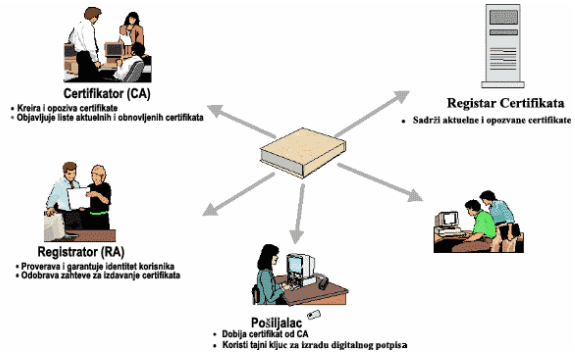
- **Verzija certifikata**
- **Serijski broj certifikata**
- **Korišćen algoritam za izradu digitalnog potpisa ( PKCS #1 HD5, RSA )**
- **Izdavač certifikata**
- **Valjanost certifikata ( od – do )**
- **Vlasnik certifikata**
- **Korišćen algoritam za šifrovanje javnog ključa ( PKCS #1, RSA )**
- **Javni ključ**
- **Vrsta certifikata ( klijent, server, osoba, preduzeće )**
- **Javni ključ izdavača certifikata**
- **Digitalni potpis izdavača certifikata**
- **Certifikat Javnog Ključa**
- 
- **Izdaje ga Certifikator nakon provere identiteta tražioca i njegovog javnog ključa**
- **Primaoc poruke može proveriti da li javni ključ pripada pošiljaocu**
- **Ako tajni ključ korisnika bude objavljen (poznat svima), vlasnikov certifikat treba opozvati**
- **Certifikator poseduje bazu podataka certifikata kao i onu opozvanih certifikata**
- **( Certificate Revocation List (CRL) )**

## Zadaci sertifikatora

- **Izdavanje certifikata**
  - **kreiranje javnog i tajnog ključa**
  - **primanje zahtjeva za izdavanje certifikata**
  - **utvrđivanje identiteta tražioca**
  - **izdavanje certifikata**
  - **upis u bazu podataka certifikata**
- **Opoziv certifikata**
  - **suspenzija ako tajni ključ bude poznat svima**
  - **ukidanje**
  - **upis u bazu podataka suspendovanih ili ukinutih**

## KO MOŽE BITI CERTIFIKATOR ?

- državna ili privatna institucija uz dozvolu države
- mogu se koristiti i usluge poznatih svjetskih certifikatora ( npr. Verisign, Thawte, ...)
- korisno je , pored certifikatora, imati registracijske ustanove ( RA ) koje obavljaju
  - Prikupljanje zahtjeva tražioca certifikata
  - Provjera opravdanosti izdavanja certifikata
  - Provjera podataka tražioca
  - Davanje mišljenja certifkatoru o izdavanju certifikata




## ZAHTJEVI SIGURNOSTI

- MEĐUSOBNA IDENTIFIKACIJA POSLOVNIH PARTNERA
- ZAŠTITA DOKUMENATA OD UNIŠTENJA ILI NEDOZVOLJENOG KORIŠĆENJA
- NEMOGUĆNOST ODBIJANJA POSLATOG DOKUMENTA
- JEDNOSTAVNOST KORIŠĆENJA