SMART KARTICE
generisanje i primjena

Sadržaj predavanja

- Istorija
- Domeni primjene
- Tehničke karakteristike
- Primjena u zdravstvu
- U vojsci
- Pasoši
- Lične karte
- Kante za smeće
- Potrebna tehnologija
- Digitalni potpis
- Digitalni sertifikat

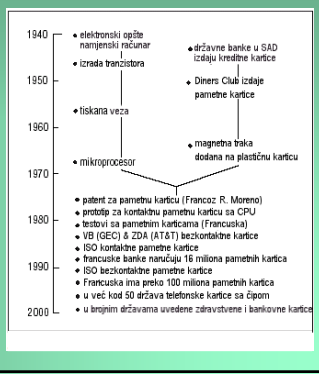
BIG BROTHER IS WATCHING YOU???

Evolucija smart kartice

PREDISTORIJA

NASTANAK

ISTORIJA



Evolucija smart kartice

- **1970**. Japanac dr Kunitaka Arimura patentira smart card koncept.
- **1974**. Francuz Ronald Moreno patentira čip-karticu, tzv. IC card, kasnije nazvanu “smart card”.
- **1977**. Tri proizvođača, Bull CP8, SGS Thomson i Schlumberger, započunju razvoj IC-ja.
- **1979**. Motorola proizvodi prvi mikrokontroler za upotrebu u francuskom bankarstvu.

Evolucija smart kartice

- **1982**. Prvo testiranje memorijske telefonske kartice u Francuskoj.
- **1984**. Uspješno završen pilot projekat ATM bankarskih čip-kartica.
- **1986**. 14000 kartica s Bullovim CP8 čipom podijeljeno je klijetima Bank of Virginia i Maryland National Bank.
- Takođe 50000 Casio kartica podijeljeno je klijentima First Nacional Palm Beach Bank i Mall Bank.
- **1987**. Prva značajna smart card aplikacija (Peanut Marketing Card) implementirana u SAD-u, Ministarstvo poljoprivrede (Department of Agriculture).

Evolucija smart kartice

- **1991**. Prvi projekat pametne kartice, Electronic Benefits Transfer (EBT), lansiran za posebni dodatni prehrambeni program u Wyomingu (Wyoming Special Supplemental Nutrition Program).
- **1992**. Nacionalni prepaid projekat DANMONT (elektronski novčanik) lansiran u Danskoj.
- **1993**. Pilot projekat multiaplikacijske smart kartice u Renneu, u Francuskoj. Funkcija javne telefonije uključena u Smart Bank Card.

7

Evolucija smart kartice

- **1994**. EuroPay, MasterCard i Visa (EMV), objavili zajedničku specifikaciju za globalnu finansijsku smart karticu.
- Njemačka započela izdavanje 80 miliona zdravstvenih memorijskih čip-kartica.
- **1995**. Smart kartice u više od 3 miliona digitalnih mobilnih telefona.
- Započelo izdavanje 40000 aplikacijskih MARC čip-kartica američkim marincima na Havajima.

8

Evolucija smart kartice

- **1996**. Više od 1.5 miliona Visa Cash kartica izdato za potrebe Olimpijskih igara u Atlanti.
- **1997**. Postavljeni standardi zbog problema interoperabilnosti smart kartica.
- Java Card podržava Visa, a MULTOS (Multi Application Operating Sistem) MasterCard.

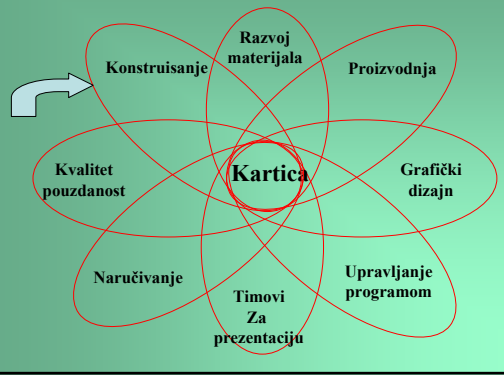
9

Evolucija smart kartice

- **1998**. Američka vlada i mornarica udružile snage u implementaciji 9-aplikacijskog sistema pametnih kartica u Centru za Smart Card Tehnologije (Smard Card Tehnology Center) u Washingtonu.
- Microsoft predstavio novi operativni sistem Windows smart card.
- Francuska započela pilot projekat zdravstvenih kartica za svojih 50 miliona stanovnika.
- **1999**. Američka vlada započela program Smart Access Cammon ID Card, za identifikaciju, fizički i logički pristup za sve zaposlene u federalnoj službi.
- Iste je godine američka vlada (General Services Administration) započela multiaplikacijski pilot projekat za Java card u Washingtonu.

10

Materijali kartica
Kvalitet, testiranje i razvoj

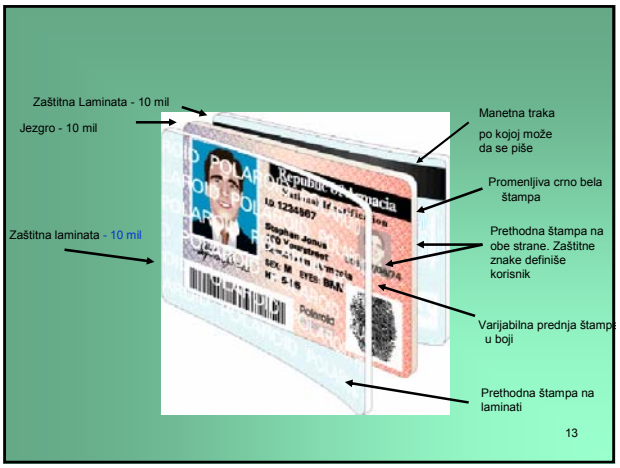


11

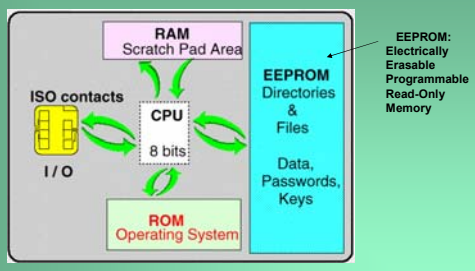
ISO 7810: ID-1 kartica

- Temperatura: 23C+/- 3C
- Vlažnost: 40% do 60%
- Debljina kartice: 0.76mm+/-0.08mm
- Materijal: PVC, Polivinilhlorid acetat, Poliester, Polietilen, Polikarbonati, Poliolefin
- Otporna na vatru
- Tempetarure testiranja: -35C do 50C
- Vlažnost: 5% do 95%
- Standardima nije predvidjena dužina trajanja kartice

12



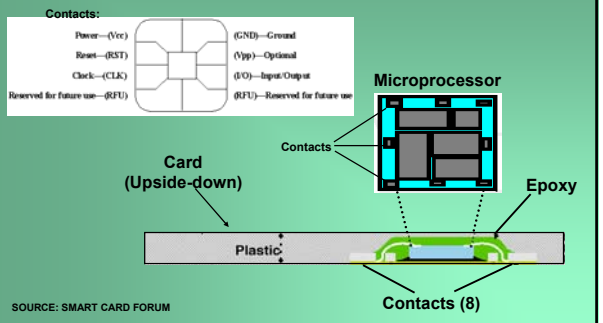
Old Smart Card Architecture



SOURCE: SMART CARD FORUM

14

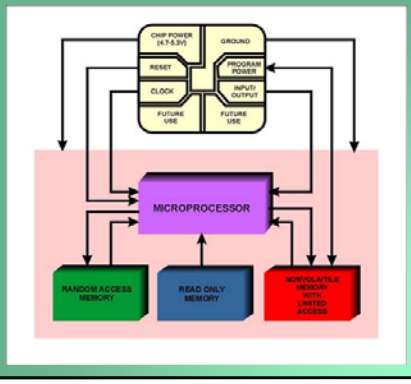
Smart Card Structure



SOURCE: SMART CARD FORUM

15

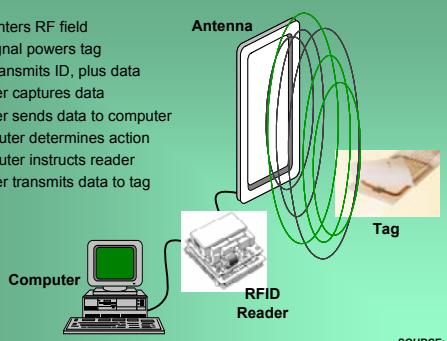
SMART CARD STRUKTURA



16

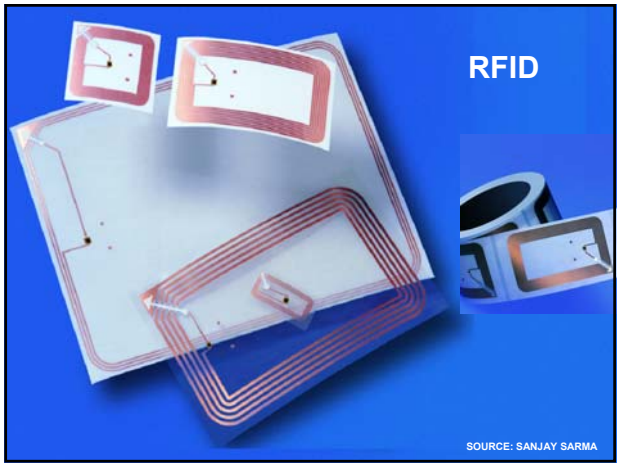
How RFID Works

- Tag enters RF field
- RF signal powers tag
- Tag transmits ID, plus data
- Reader captures data
- Reader sends data to computer
- Computer determines action
- Computer instructs reader
- Reader transmits data to tag



SOURCE: PHILIPS

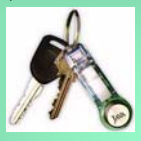
17



Java Ring

- Java-enabled iButton
- Communicates by contact at 142 Kbps
- 64 KB ROM and 134 KB RAM
- Stores 30 digital certificates with 1024-bit keys
- Uses: authentication, epayment, access
- Cost: $15-30 in unit quantity






SOURCE: IBUTTON.COM

Multi-Application Smart Card

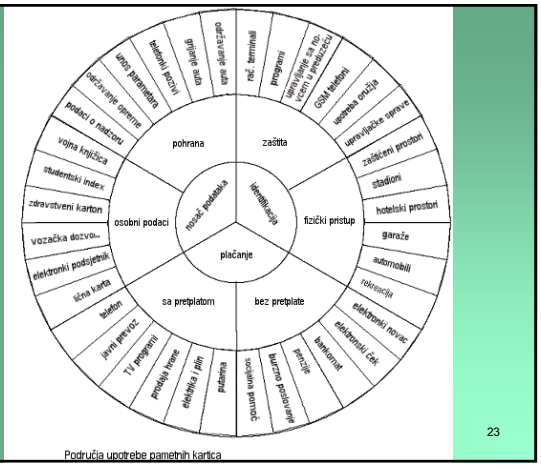
SOURCE: SECURITY DYNAMICS

Domeni primjene

- Financijske
- - Elektronski novčanik - zamjenjuje gotovinu (npr. kovanice u automatima) i služi za plaćanje manjih iznosa
- - Kreditne i debitne kartice - zamjenjuju postojeće magnetske kartice, pružajući veću sigurnost i mogućnost offline i semi-online transakcija
- - Sigurno plaćanje putem Interneta
- Komunikacije
- - Sigurno započinjanje razgovora i identifikacija inicijatora komunikacije (za potrebe naplate poziva) u mobilnim mrežama, roam-ing, SMS usluge, m-commerce
- - Telefonske prepaid kartice
- - Pretplata za televizijske programe
- Information Security
- - Zaštićeni pristup zaposlenih računarskim mrežama u kompanijama s mogućnošću primjene biometrijskih metoda
- Fizički pristup
- - Kartice za pristup zaposlenih određenim fizičkim objektima (mogućnost primene biometrije), kontrola radnog vremena, korištenje kantine...

Domeni primene

- Transport
- - Vozačke identifikacijske dozvole
- - Plaćanje voznih karata u masovnom prevozu
- - Elektronska naplata putarine
- Trgovina
- - Praćenje kupovine pomoću loyalty sistema radi nagrađivanja vernih kupaca, zadržavanja novih, analiziranja potreba kupaca, a time i povećanja tržišta i profita
- Zdravsto
- - Kartice zdravstvenih osiguranika koje sadrže najvažnije zdravstvene podatke, smanjuju administrativne troškove i mogućnosti pronevjere
- Univerzitetske identifikacione kartice
- - Višenajmenske, primer elektronski novčanik, korišćenje indeksa, ishrana, pranje odjeće, pristup objektima...



Područja upotrebe pametnih kartica

Čitači smart kartica

USB čitač smart kartica

Čitači smart kartica

25

Prednosti

- Višefunkcionalnost
- Pojeftinjenje novčanih transakcija, umesto materijalnog novca koristi se elektronski novac pohranjen u digitalnom obliku u karticama;
- Pojednostavljenje toka transakcija, smanjenje količine materijalnog novca u opticaju čime se pojednostavljuje rukovanje njime;
- Značajno se smanjuje mogućnost krađe ili zloupotrebe pametnih kartica sa skladištenim novčanim vrednostima, naročito kada je upotrebljena PIN (*Personal Identification Number*) metoda identifikacije prije transakcije;
- Za razliku od magnetskih kartica gdje su podaci na površini i lako dostupni oštećivanju i provali, kriptovanom digitalnom sadržaju pametnih kartica je gotovo nemoguće neovlašteno pristupiti radi čitanja ili menjanja sadržaja;

26

Prednosti

- Same kartice i lični uređaji koje korisnik treba imati su relativno jeftini;
- Anonimnost korisnika tokom transakcije zagarantovana;
- Visoka deljivost sredstava sa kartice omogućena samom digitalizacijom novčanih vrednosti;
- Mogućnost višefunkcijskih kartičnih sistema, koji bi pružili mogućnost upotrebe iste kartice za više namena, na primer
  - skladištenje novčanih vrednosti,
  - plaćanje javnog prevoza,
  - telefona,
  - sadržavanje različitih ličnih podataka,
  - identifikaciju digitalnim potpisom i sl.

27

Nedostatci

- Kriptografski algoritmi stari preko 10 godina,
- Osjetljive na vlagu,
- Osjetljive na temperaturu,
- Osjetljive na mehanička oštećenja

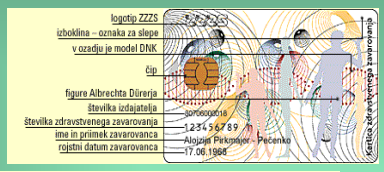
28

Kartica u zdravstvu - primena u Sloveniji

- Kartica zdravstvenog osiguranja je jedini važeći dokument za ostvarivanjenje prava i obaveza iz dobrovoljnog zdrastvenog osiguranja u Sloveniji.
- Taj elektronski lični dokumenat su uzeli svi koji imaju obavezno zdravstveno osiguranje u Sloveniji, to je oko 2 miliona ljudi.
- U primeni su dvojezične kartice i to: 1. na slovenačkom i italijanskom i 2. slovenački i mađarski.
- Valjanost zdrastvenog osiguranja potvrđuje svako sam na samouslužnim terminalima, preko kojih iz centralnih baza se zapisuju na karticu najnoviji podaci.
- Kartica zdravstvenega osiguranja je mikroprocesorska kartica s 16 kB prostora.

29

Kartica u zdravstvu - primena u Sloveniji



30

Vidljivi podaci - pacijent

- O imaocu kartice (ime i prezime, naslov, pol, datum rođenja);
- O korisniku premije (registracioni broj, naziv, naslov);
- O obveznom zdravstvenem osiguranju (datum početka i trajanje osiguranja);
- O postojećem zdravstvenm osiguranju (vrsta polise, trajanje osiguranja);
- O izabranom ličnom ljekaru (ljekar opšte prakse / pedijatar, zubar, ginekolog).

31

Digitalni podaci - lekar

- ZZZS broj imalaca,
- Broj izvoda kartice,
- Ime i prezime imaoca,
- Šifra države,
- Specializacija i tip oblasti.

32

Čitači smart kartice

Američka vojska i smart kartice

- Američka vojska predstavila je javnosti novu generaciju "pametnih" identifikacionih kartica, koje će uz sebe ubuduće nositi
- Više od četiri miliona vojnika, uključujući aktivno vojsku,civile zapošljene pri oružanim snagama te ljudima iz pojedinih firmi koje uže sarađuju s američkim Ministarstvom obrane.
- Identifikacione kartice za američke vojnike postupno će biti uvedene tokom sedećih petnaestak mjeseci.
-

34

Američka vojska i smart kartice

- Svaka vojna pametna kartica sastoji se od
  - digitalizovane fotografije,
  - linijskog koda,
  - magnetne trake i
  - identifikujućih tekstualnih podataka,
- Svrha će im biti pre svega:
  - povećanje sigurnosti te veća zaštita pristupa do 900 američkih vojnih postrojenja širom svijeta, među kojima su, naravno, Pentagon, infrastruktura vojnih kompjuterskih mreža, a
  - služiće i za korespondenciju šifriranim porukama e-pošte, pa čak i za
  - finansijske online transakcije pripadnika američkih oružanih snaga.
-

35

Američka vojska i smart kartice

- Vojne pametne kartice zasad neće nositi medicinske podatke o svom nosiocu, već će se koristiti kao siguran pristupni dokument tim podacima smještenim u vojnim kompjuterima.
- Pentagon je još dosta neodlučan, kako zbog sigurnosnih, tako i zbog razloga zaštite privatnosti pojedinaca zaposlenih u američkoj vosjci.

36

Pametni pasoši

- Britanci bi uskoro mogli dobiti "pametne" pasoše, u kojima bi bili smešteni otisci prstiju i drugi lični podaci. "Pametni" pasoši, bili bi uvedeni u periodu od četiri godine, takodje bi bili biometrijske kartice sa čipom.
- Na karticama bi bile sačuvane digitalne slike vlasnika, skenirane slike zenica očiju i otisci prstiju.
- Kartice bi još izvjesno vrijeme dopunjavale uobičajene papirne pasoše, zbog toga što se mnoge zemlje jos uvijek oslanjaju na stari sistem stavljanja pečata kao potvrde da je osoba prešla granicu.
- Lične kartice koje su predlozene čuvale bi podatke o obrazovanju, zdravstvenom i socijalnom osiguranju korisnika, a za njihovu izradu bi se koristila tehnologija koja je već u upotrebi.
- Naime, od 31. januara ove godine, svi oni koji traze azil u Velikoj Britaniji dobijaju biometrijske kartice.

37

Digitalna lična karta

- Građani britanskog grada **Bracknell**-a od januara 2001. godine mogu da koriste javne servise i usluge na potpuno nov način.
- Svaki od 110.000 stanovnika može da dobije digitalni identitet i da koristi web u svrhu interakcije sa lokalnim vlastima i ustanovama.
- Oni koji se odluče za digitalnu "ličnu kartu" će moći da plaćaju porez, komentarišu odluke lokalnih vlasti, saznaju detalje o radu direkcije za stambeno i građevinsko zemljište.
- Sve ono što je inače dostupno samo ako se zakuca na vrata određene kancelarije, sa novim će sistemom biti na samo klik od korisnika.
- Ovakav plan gradskih vlasti u Bracknell-u se uklapa u projekat britanske vlade koji bi trebao da do 2005. godine omogući pristup i korišćenje svih lokalnih servisa putem Interneta.

38

Digitalna lična karta

- U budžetu za 2001. godinu je čak 350 miliona funti izdvojeno za takve namjene i ta suma je raspodijeljena britanskim opštinama.
- Što se tiče grada Bracknell-a, cilj tamošnjih vlasti je da svaki od 110.000 stanovnika dobije svoj digitalni identitet u obliku korisničkog imena i lozinke pomoću kojih će moći da koriste brojne servise.
- Prednosti su očigledne - po informacije se ne mora ići na lice mjesta, niti se mora voditi računa o radnom vremenu, jer je sve dostupno 24 časa na dan.
- Lokalne vlasti i očekuju da će se, na ovaj način, povećati efikasnost gradskih službi, pa samim tim i zadovoljstvo i kvalitet života građana.
- Oni će moći da putem Interneta prijavljuju neispravnu uličnu rasvjetu, oštećene saobraćajne znakove, nove grafite, polomljene klupe i, uopšte, sve ono što ne valja ili što treba popraviti.

39

Pametne kante za smeće

- Na ovom svijetu je sve više pametnih stvari - pametna odeća, pametne kartice, a uskoro će postojati i pametne kante za smeće.
- Pridjev "pametno" u svim ovim slučajevima znači da je stari, dobro poznati predmet, obogaćen novom tehnologijom, odnosno da mu je ugrađen procesor koji donosi potpuno nove mogućnosti.
- Što se tiče usavršenih kanti, one će se pojaviti na ulicama Barselone, pri čemu će ugrađeni mikroprocesori mjeriti količinu smeća i pratiti kada je poslednji put kanta ispražnjena.
- Radnici gradske čistoće u ovom gradu će uz pomoć prenosivih kompjutera pratiti podatke o svakoj kanti i nadgledati statistike o tome koliko se često ona puni, kada je zadnji put ispražnjena, kada je zadnji put prefarbana.
- Podaci će se obrađivati uz pomoć posebnog softvera, pri čemu gradske vlasti smatraju da će na ovaj način postići racionalnije korišćenje svojih "resursa" za odlaganje smeća.
- U prvoj fazi ovog projekta biće postavljeno 600 takvih kanti u stari dio grada, a sledeći korak predstavlja potpuna kompjuterizacija svih 20.000 kanti i kontejnera u ovom gradu.

40

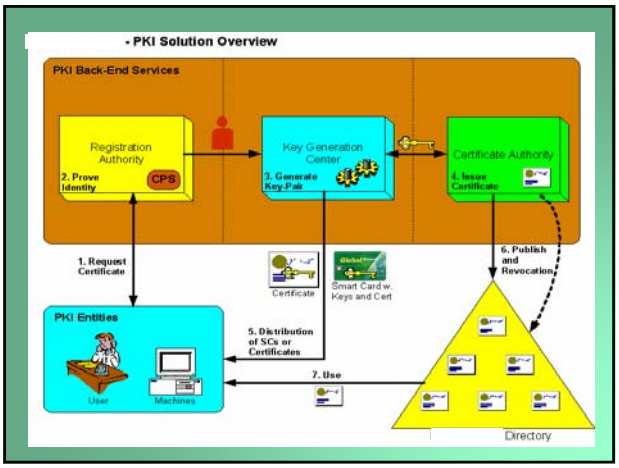
Potrebna tehnologija

- Zakonska regulativa
- Sertifikaciono telo
- Zakon o digitalnom potpisu

41

Sertifikat autoritet

42



PKI pozadinski servisi

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

44

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).

45

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).

46

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.

47

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.

48

Trajanja važnosti sertifikata (validity period)

- Smeštaj 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.

49

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.

50

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.

51

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.

52

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 saobračaj.
- ·**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.

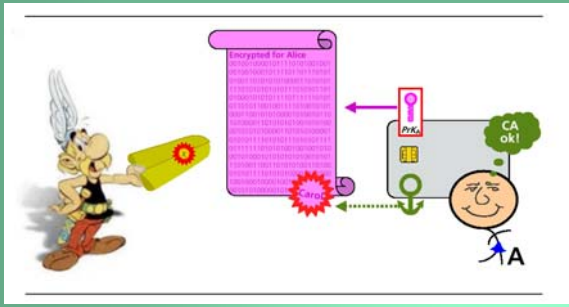
53

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.

54

ELEKTRONSKI POTPIS



55

ELEKTRONSKI POTPIS

- niz znakova u elektronskom obliku
- kreiran računarom
- ima istu pravnu snagu kao ručni potpis
- često se poistovjećuje sa digitalnim potpisom

56

TEHNOLOGIJE ELEKTRONSKOG I DIGITALNOG POTPISA

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

57

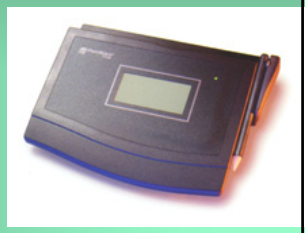
SKENIRANI RUČNI POTPIS

- 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

58

Tabla za potpis

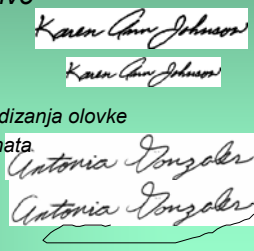
- Potpisnik potpisuje tablet specijalnom olovkom
- Softver koriguje pukotine u potpisu tako da ja neprekidan
- I invalidi mogu da koriste ovaj uredjaj



59

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*

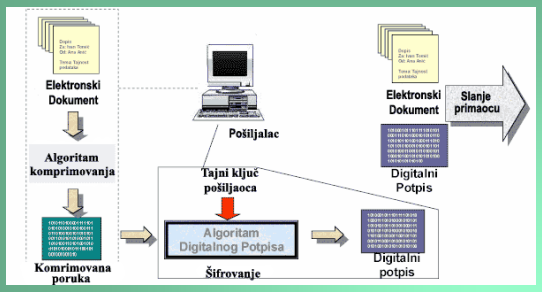
60

DIGITALNI POTPIS

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

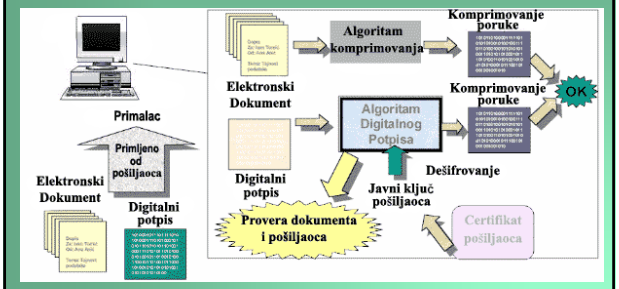
61

Kreiranje digitalnog potpisa



62

Provjera digitalnog potpisa



63

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@UuhX2soUspaufVsfopSu8tby1kUXTGsFhAgsEYa0/eed9+59917j3nsS17746789Retyiop47987HgiuopŠtrvgui0456/ajW/7rllBrj/ZbfWrtopHGz467/opšthikkuekopBV562Rmj2nd Frt1d8dNmyvvq12K7tj89opLxf**
- **--- END PGP SIGNATURE ---**

64

POMOĆU CERTIFIKATA PRIMALAC

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

65

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))**

66

Zadatci sertifikatora

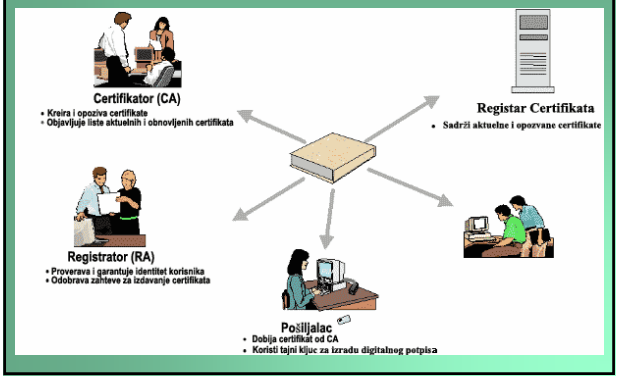
- **Izdavanje certifikata**
  - **kreiranje javnog i tajnog ključa**
  - **primanje zahtjeva za izdavanje certifikata**
  - **utvrđivanje identiteta tražioca**
  - **izdavanje certifikata**
  - **upis u bazu podataka certifikata**
- **Opoziv certifikata**
  - **suspenzija ako tajni ključ bude poznat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

67

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

68



ZAHTJEVI SIGURNOSTI

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

70

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,

71

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.

72