HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Smart Card sigurnosni sustavi

CCERT-PUBDOC-2004-03-65

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.
Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr**- laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Smart kartica (eng. *smart card*) je plastična kartica veličine standardne kreditne kartice koja u sebi sadrži mikročip. Ugrađeni mikročip, osim što može služiti kao memorija za pohranjivanje podataka, može obavljati i neke logičke operacije nad tim podacima. Rane smart kartice sadržavale su mikročip koji je služio samo kao memorija, dok današnje kartice imaju funkcije mini računala, tj. na sebi sadrže jednostavni operacijski sustav i nekoliko neovisnih aplikacija.

Bitno svojstvo smart kartica je samodostatnost, tj. neovisnost o vanjskim resursima, što je čini izuzetno otpornom na potencijalne napade. Baš zbog ovog svojstva smart kartice su postale često korišten instrument osiguranja u aplikacijama koje zahtijevaju visok nivo sigurnosne zaštite, te u procesima autentikacije za dokazivanje identiteta vlasnika.

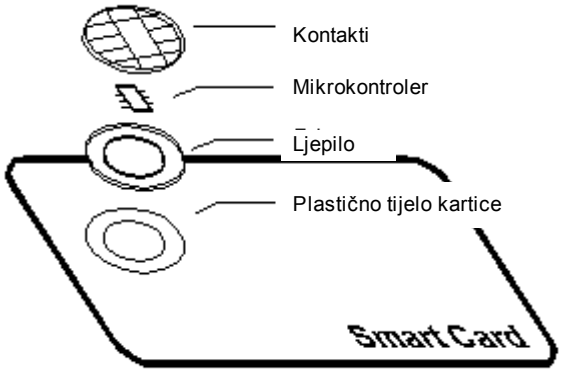
Isto tako, osim za identifikaciju, smart kartica može služiti i za pohranjivanje osobnih medicinskih podataka, a već se koristi za identifikaciju korisnika i obavljanje financijskih transakcija između korisnika i banaka. Smart kartice svakim danom postaju sve važnije i igrati će veliku ulogu u svakodnevnom životu u budućnosti, kada će pohranjivati mnogo više povjerljivih podataka nego što to danas čine klasične magnetske kartice, pa samim tim pitanja sigurnosti smart kartica i podataka koje one pohranjuju postaju predmetom velikog interesa.

U ovom dokumentu razmatra se sigurnost samih smart kartica, ali i sigurnost koju smart kartice zbog svojih svojstava mogu dati aplikacijama koje ih koriste. Na samom početku obrađena je fizička struktura smart kartice te zaštita podataka koja se ostvaruje strukturom same kartice. Zatim je opisana zaštita podataka na smart kartici putem logičkih kontrola pristupa podacima na kartici, kao i mehanizmi enkripcije podataka, dok se u zadnjem dijelu dokumenta daje prikaz metoda i mehanizama u kojima se smart kartica koristi za osiguravanje sigurnog okruženja za izvršavanje raznih aplikacija.

2. Struktura i životni vijek smart kartice

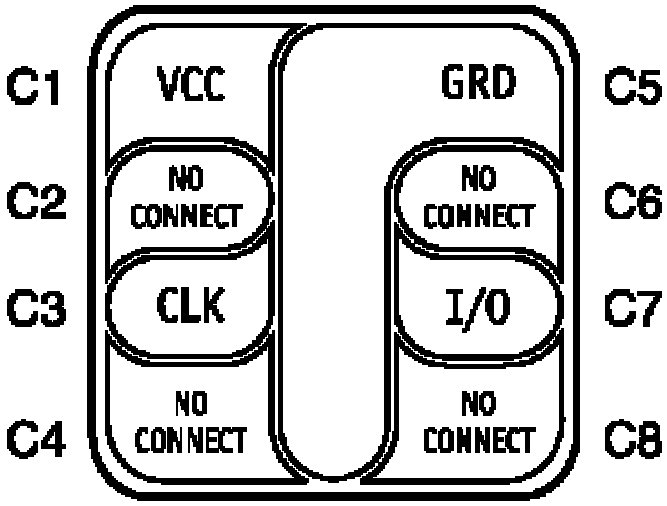
2.1. Fizička struktura

Fizička struktura smart kartice definirana je ISO standardima 7810, 7816/1 i 7816/2. U osnovi smart kartica sastoji se od 3 glavna elementa – plastične podloge dimenzija 85.60mm x 53.98mm x 0.80mm, metalnih kontakata i mikročipa ugrađenih u plastičnu podlogu.



Slika 1: *Fizička struktura smart kartice*

Raspored i funkcija metalnih kontakata određeni su ISO standardom 7816/3 koji definira 5 konekcijskih točaka za ostvarivanje napajanja i prijenos podataka između terminala i kartice.



Slika 2: *Raspored kontakata smart kartice prema ISO 7816/3*

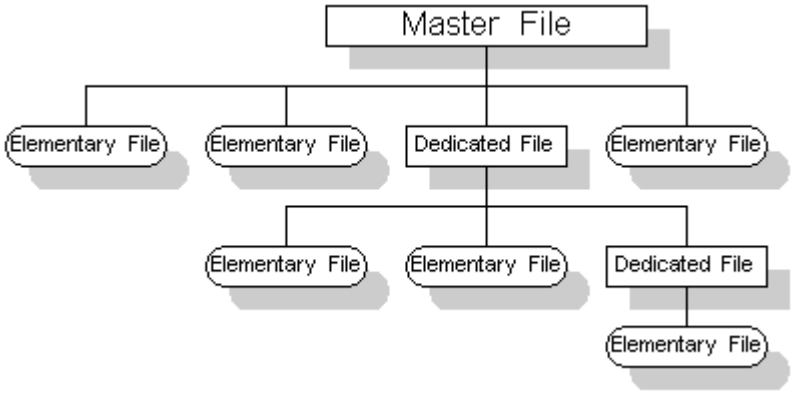
Karakteristike smart kartice određene su ugrađenim mikročipom koji se sastoji od mikroprocesora, ROM memorije, dinamičke radne memorije i električno programibilne ROM memorije (EEPROM) koja zadržava svoje stanje i nakon uklanjanja napajanja. Mikročipovi koji se danas ugrađuju napravljeni su od silicija koji nije fleksibilan i lako je lomljiv, pa se, da bi se izbjeglo njihovo lomljenje prilikom savijanja kartice, veličina tih mikročipova reducira na svega nekoliko milimetara.
Fizičko sučelje koje omogućava razmjenu podataka između kartice i terminala ograničeno je na 9600 bit/s putem serijske komunikacije koja je također specificirana ISO standardom 7816/3. Komunikacija

je *semi-duplex* tipa, tj. prijenos podataka se može provoditi u oba smjera, ali ne u isto vrijeme, a kontrolu komunikacije vrši sam mikročip. Komunikacija se sastoji od komandi i ulaznih podataka koji se šalju mikročipu na kartici, koji zatim na njih odgovara izvješćima o statusu i izlaznim podacima. Format komandi i ulazno/izlaznih podataka opisan je specifikacijama komunikacijskih protokola T=0 (*asynchronous half-duplex character transmission protocol*) i T=1 (*asynchronous half duplex block transmission protocol*) koji su također dio ISO standarda 7816/3. Upotrebom ovih specifičnih protokola i ograničenjem brzine prijenosa podataka značajno se smanjuju mogućnosti napada na sadržaj kartice.

2.2. Logička struktura

Nakon što je smart kartica izdana korisniku, zaštita kartice zasniva se na operacijskom sustavu s kojim je kartica isporučena. Fizičko adresiranje memorije i podataka na kartici više nije moguće, već se njima pristupa putem logičke strukture datoteka. Operacijski sustav koji omogućava takvu organizaciju datoteka ujedno omogućava i kontrolu pristupa svakoj od njih, te na taj način određuje koji podaci su kome dostupni.

Općenito gledajući iz perspektive pohrane podataka, smart kartica je slična tvrdom disku i također je organizirana hijerarhijski u obliku direktorija. Slično kao kod MS-DOS operacijskog sustava postoji jedna master datoteka MF (eng. *Master File*) koja je ekvivalent root direktoriju. Unutar root direktorija nalaze se datoteke koje se nazivaju elementarne datoteke EF (eng. *Elementary File*), kao i pod-direktoriji DF (eng. *Dedicated File*), koji opet mogu sadržavati elementarne datoteke. Razlika prema MS-DOS je u tome što pod-direktoriji mogu sadržavati i same podatke, a ne samo datoteke. Primjer takve strukture prikazan je na sljedećoj slici.



Slika 3: *Struktura datoteka smart kartice*

Općenito gledajući, struktura datoteka operacijskog sustava na smart kartici slična je strukturi drugih operacijskih sustava kao što su MS-DOS ili UNIX, no da bi se povećala sigurnost sustava definiraju se sigurnosni atributi za svaku datoteku. Ti sigurnosni atributi sadrže informacije o uvjetima pristupa datoteci kao i polja za indikaciju statusa datoteke. Također je definirana i takozvana sigurnosna brava datoteke koja se koristi za potpuno onemogućavanje pristupa datoteci. Ovi sigurnosni mehanizmi predstavljaju sustav logičke zaštite smart kartice.

3. Sigurnosni mehanizmi

3.1. Logička zaštita

Sigurnosni mehanizmi smart kartice odnose se uglavnom na kontrolu i ograničavanje pristupa datotekama na smart kartici. Spomenuti mehanizmi baziraju se na sigurnosnim atributima opisanim u prethodnom poglavlju. Rad sigurnosnih atributa zasniva se na ispravnoj prezentaciji sigurnosnog koda (PIN kod) kartice i upravljanju tim kodom.

Prema prezentaciji PIN koda definira se 5 kategorija uvjeta pristupa datotekama koje osigurava operacijski sustav smart kartice (treba napomenuti da neki operacijski sustavi mogu ponuditi i dodatne nivoe, ovisno o aplikaciji za koju se sama kartica koristi):

1. Uvijek - ALW (eng. *Always*) – ne postoji ograničenje pristupa datoteci;
2. Verifikacija vlasnika kartice 1 – CHV1 (eng. *Card Holder Verification 1*) – pristup datoteci samo uz prezentaciju važećeg CHV1 (PIN kod 1);
3. Verifikacija vlasnika kartice 2 – CHV2 (eng. *Card Holder Verification 2*) – pristup datoteci samo uz prezentaciju važećeg CHV2 (PIN kod 2);
4. Administrativni – ADM (eng. *Administrative*) – kriterije prava pristupa datoteci definira administrator koji dodjeljuje taj nivo sigurnosti određenoj datoteci;
5. Nikad – NEV (eng. *Never*) – pristup datoteci je zabranjen.

Ove kategorije, međutim, nisu hijerarhijske. Tako npr. prezentacija važećeg CHV2 ne podrazumijeva pristup datoteci koja za pristup zahtijeva prezentaciju važećeg CHV1, već se njoj pristupa samo prezentacijom važećeg CHV1. To znači da se određenoj datoteci može pristupiti samo uz zadovoljenje specifičnih uvjeta pristupa definiranih za tu datoteku.

CHV1 i CHV2 obično su pohranjeni u odvojenim elementarnim datotekama npr. EF_{CHV1} i EF_{CHV2} i prava pristupa tim datotekama sprječavaju ili omogućavaju njihovu promjenu uz određene uvjete.

3.2. Aplikacijska zaštita

Osim fizičke i logičke zaštite koje pruža sama smart kartica, zbog procesorskih mogućnosti koje posjeduje u nju ugrađeni mikročip smart kartica može pružiti zaštitu podataka i na aplikacijskom nivou. Na primjer, smart kartica i kartični terminal mogu međusobno putem autentikacijskih procedura (*challenge* protokol) provjeriti identitet druge strane. Isto tako, procesorske mogućnosti omogućavaju implementaciju kompleksnih enkripcijskih funkcija na samu karticu, tako da sva komunikacija s vanjskim jedinicama bude zaštićena enkripcijskim kodom koji je nemoguće ili vrlo teško probiti. U tom slučaju enkripcijski ključevi koji su pohranjeni u datoteke na kartici koriste se kao osnova za enkripcijske algoritme koji se u obliku programskog koda izvršavaju na ugrađenom procesoru kartice. Ukoliko se na kartici nalazi više aplikacija, za svaku od njih može se primijeniti zaseban enkripcijski ključ tako da proboj jedne aplikacije ne znači automatski i proboj svih ostalih.

Neki tipični enkripcijski algoritmi koji se primjenjuju na današnjim smart karticama i njihova primjena navedeni su u tabeli 1.

Algoritam	Upotreba
DES	Komunikacijski kanali
A3 i A8	GSM SIM kartice
Elliptic curve	Digitalni potpis (eng. *Digital signature*)
TSA7	Zdravstveni/medicinski podaci
RSA	Digitalni potpis

Kolika je sigurnost podataka koji su pohranjeni na kartici te koliko je sigurna komunikacija kojom se ti podaci prenose s kartice na terminal i obratno, ovisi o sigurnosti enkripcijskih algoritama i metoda koje se primjenjuju, ali u svakom slučaju nivo sigurnosti je znatno povećan. Osim toga, pošto se radi o softverskoj zaštiti, implementacijom novih algoritama kako se oni budu pojavljivali nivo sigurnosti i zaštite podataka na kartici može se vrlo jednostavnim nadogradnjama softvera još povećati prema potrebi.

4. Primjena - sigurnosne aplikacije

Zbog sigurnosti pohranjenih podataka i autonomnosti koju posjeduje, smart kartica se često koristi kao sastavni dio sigurnosnih aplikacija pri čemu se najosjetljiviji podaci i algoritmi pohranjuju ili izvršavaju na samoj kartici. Primjer takve aplikacije je sustav u kojem se smart kartica na kojoj se pohranjuje ili generira korisnički ključ upotrebljava za autorizaciju pristupa računalu i tako zamjenjuje klasičnu autorizaciju pristupa putem korisničkog imena i zaporke. Drugi primjer integracije smart kartice u sigurnosnu aplikaciju je zaštita dokumenata digitalnim potpisom koji se putem određenih procedura, koje se dijelom izvršavaju na smart kartici, integrira u elektronski dokument štiteći ga tako od falsificiranja. Kako izgledaju takvi sustavi i zašto oni garantiraju veću sigurnost biti će opisano u sljedećim poglavljima.

4.1. *Digital signature* za zaštitu dokumenata

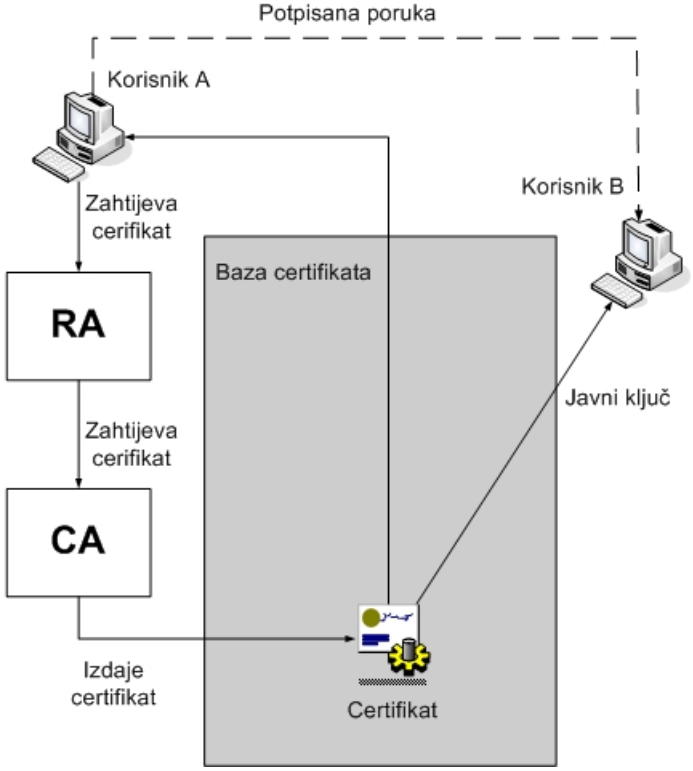
Za zaštitu podataka u mrežnoj komunikaciji najlakše je primijeniti enkripciju podataka.
Kod simetrične enkripcije podataka problem predstavlja razmjena ključeva koji se koriste za enkripciju i dekripciju podataka. Kako se za oba postupka koristi isti ključ, pošiljatelj poruke mora primatelju poslati ključ s kojim je poruka enkriptirana. Ako je taj ključ potrebno poslati preko računalne mreže, sigurnost takvog ključa postaje problem.
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 (koji se naziva 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 kojem je namijenjena, a sigurnost ključa nije upitna. Usprkos ovoj očiglednoj prednosti, asimetrična enkripcija se rijetko koristi jer je algoritam puno sporiji od simetrične enkripcije.
Kako bi imali prednosti oba opisana sustava, 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 simetrični ključ zaštićen u komunikacijskom kanalu, a za dekripciju poruke je moguće koristiti brži algoritam.
Ovakvi sustavi omogućuju i digitalni potpis dokumenata. 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 danas poznatim 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 je li dokument promijenjen negdje unutar 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 sam generirao iz primljenog dokumenta. Ako su sažeci jednaki onda je sigurno da ga je poslao deklarirani pošiljatelj i dokument sigurno nije u međuvremenu promijenjen.
Iz opisanih postupaka za zaštitu dokumenata vidljivo je da sigurnost komunikacije ovisi o vjerodostojnosti javnog ključa korisnika te da taj ključ mora biti poznat velikom broju korisnika. Osobe koje žele komunicirati mogu prije toga same razmijeniti javne ključeve, ali to u raširenoj poslovnoj komunikaciji nije praktično. Puno bolje rješenje je pohrana javnih ključeva u nekom javnom mrežnom direktoriju gdje svatko može pronaći i skinuti ključ osobe s kojom želi komunicirati (poput telefonskog imenika).
Poznavanje javnog ključa ne omogućuje dekripciju dokumenata pa javni ključ može biti svima poznat. Međutim javni ključ je moguće lažirati i na taj način presresti i dekriptirati poruke pa se zbog toga pojavljuje problem vjerodostojnosti takvog ključa, posebno ako se javni ključ šalje preko nezaštićenog komunikacijskog kanala.
Za rješavanje tog problema primjenjuje se PKI sustav koji je opisan u slijedećem poglavlju.

4.2. PKI

PKI (eng. *Public Key Infrastructure*) je mehanizam za dodjeljivanje i sigurnu distribuciju javnih ključeva za zaštitu komunikacije. Zadaća PKI sustava je uspostavljanje povjerenja potrebnog za normalno vođenje poslovanja.

4.2.1. Princip rada PKI-a

Osnovni princip rada PKI sustava je prikazan na slici 4.



Slika 4: *Princip rada PKI sustava*

Sustav se bazira na izdavanju digitalnih certifikata sa javnim ključevima. Digitalni certifikat je posebna struktura podataka koja sadrži javni ključ korisnika, neke podatke koji određuju identitet vlasnika tog javnog ključa, identifikacijsku oznaku samog PKI poslužitelja i datum do kojeg certifikat vrijedi. Digitalni certifikat se uvijek šalje potpisan digitalnim potpisom samog PKI poslužitelja. Pretpostavka je da svi korisnici vjeruju digitalnom potpisu PKI poslužitelja (javni ključ PKI poslužitelja se može isporučiti na CD-u svakom korisniku i nema potrebe da se šalje preko mreže) pa je taj potpis garancija da je certifikat autentičan.

Svaki korisnik koji želi upotrebljavati PKI sustav za zaštitu komunikacije mora dobiti jedan ili više vlastitih certifikata. Ustanova od koje korisnik mora zatražiti certifikat je RA (eng. *Registration Authority*). RA je ustanova koja provjerava identitet korisnika (korisnik najčešće mora dokazati identitet nekim dokumentom). Nakon što RA odobri izdavanje certifikata, korisnikov zahtjev se prosljeđuje CA (eng. *Certification Authority*), ustanovi koja izdaje certifikat. PKI sustav mora imati barem jednu CA ustanovu kojoj korisnici vjeruju. Sustav uopće ne mora imati RA ustanovu (u tom slučaju CA provjerava identitet korisnika), a može ih imati i nekoliko, ovisno o veličini sustava.

Nakon što je korisniku izdan certifikat generira se par ključeva. Tajni ključ iz para pohranjuje korisnik, a javni ključ se sprema u bazu ključeva i šalje drugim korisnicima koji žele komunicirati s vlasnikom ključa.

Par ključeva može generirati CA ustanova, nakon čega se ključevi šalju korisniku (nekom sigurnom metodom kao što je uručivanje ključeva na CD-u), a javni ključ se pohranjuje u bazi ključeva. Druga (i sigurnija) metoda je da vlasnik certifikata generira ključeve i CA ustanovi pošalje samo javni ključ. Na taj način je sigurno da je samo vlasniku certifikata poznat tajni ključ.

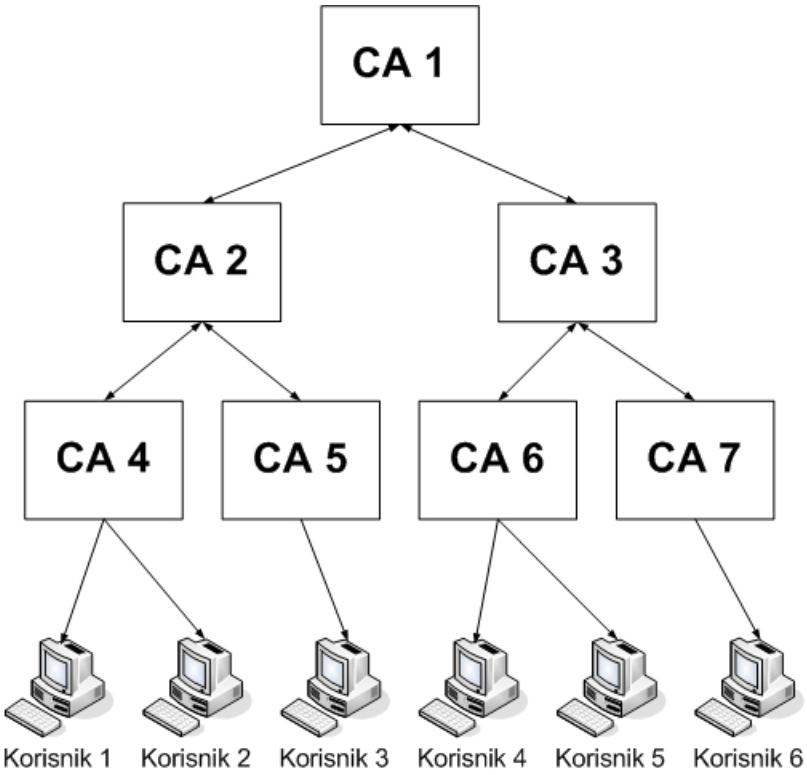
Svaki korisnik koji želi komunicirati s vlasnikom certifikata može od PKI sustava dobiti njegov certifikat sa javnim ključem.

Kako bi se osigurala što veća sigurnost dokumenata, svaki certifikat ima konačan rok valjanosti nakon čega vlasnik mora od RA ustanove zatražiti ponovno izdavanje certifikata. Na taj način se smanjuje

vrijeme koje neovlašteni korisnici imaju na raspolaganju za kriptoanalizu ključa u certifikatu ili za podmetanje lažnog ključa.

4.2.2. Struktura PKI-a

Uspješnost PKI sustava ovisi o povjerenju koje korisnici imaju u određenu CA ustanovu. Za manje PKI sustave je moguće da svi korisnici sustava vjeruju istoj CA ustanovi.
Za raširenije (ili čak globalne) PKI sustave jako je teško izgraditi CA kojem će vjerovati svi korisnici. U takvom sustavu svaki korisnik vjeruje svojoj lokalnoj CA ustanovi koja izdaje njegove certifikate, a CA tijela se moraju međusobno certificirati i nakon toga mogu razmjenjivati certifikate prema željama korisnika. CA ustanove koje se međusobno certificiraju stvaraju svojevrsnu mrežu koja najčešće ima hijerarhijsku strukturu sa glavnim CA tijelom na vrhu, zatim lokalnim CA ustanovama ispod toga i korisnicima sustava na dnu.



Slika 5: *Hijerarhijska PKI struktura*

Na slici 5 je prikazan jedan primjer takve hijerarhijske strukture PKI sustava.
Sve CA ustanove na slici su međusobno certificirane i mogu razmjenjivati korisničke certifikate potpisane digitalnim potpisom same ustanove. Na primjer, ako korisnik 5 želi provjeriti potpis dokumenta koji mu je poslao korisnik 2, mora dobiti certifikat korisnika 2. Taj certifikat izdaje CA4, ali korisnik 5 komunicira (i vjeruje) jedino s CA6. Zbog toga će traženi certifikat biti proslijeđen redom između poslužitelja CA4, CA2, CA1, CA3 i na kraju CA6.
Postoje PKI sustavi koji nemaju nikakvu određenu strukturu. U takvom sustavu bilo koji CA može certificirati bilo koji drugi CA kojem vjeruje i na kraju se stvara razgranata mreža u kojoj svaki poslužitelj vjeruje onom susjednom. Takva mreža se naziva mreža povjerenja (engl. *Web of Trust*).
PGP sustav za zaštitu mrežne komunikacije koristi PKI sustav za razmjenu javnih ključeva koji ima strukturu mreže povjerenja. U PGP sustavu svaki korisnik može postati CA autoritet za certificiranje drugih ključeva. Cijeli sustav se bazira na povjerenju koje jedni korisnici imaju u druge.

4.2.3. Primjena smart kartica

Smart kartice poboljšavaju nivo sigurnosti mrežne komunikacije koji omogućuje PKI sustav. Smart kartice se u ovom slučaju primjenjuju za pohranjivanje korisničkih tajnih ključeva. Tajni ključ je obično

dugačak pseudo-slučajni niz koji je gotovo nemoguće zapamtiti i upisivati svaki puta kada ga korisnik želi upotrijebiti. Zbog toga ključ mora biti fizički pohranjen na korisničkom računalu. Takva pohrana ključa je velika sigurnosna rupa u sustavu jer su korisnička računala obično slabo zaštićena od napada raznih crva koji neovlaštenim korisnicima omogućuju čitanje tako pohranjenog tajnog ključa.
Ako je tajni ključ pohranjen na smart kartici nemoguće ga je pročitati, a osim toga, smart kartica omogućuje sigurni medij za slanje para ključeva vlasniku certifikata.

5. Zaključak

U dokumentu je opisana struktura smart kartica te glavni načini njihove primjene. Smart kartice omogućavaju izgradnju sustava za autentikaciju korisnika s dosad nezamislivom razinom modularnosti, samodostatnosti, sigurnosti, nadogradivosti, jednostavnosti i funkcionalnosti.

Smart kartice imaju sve širu primjenu i sve više zamjenjuju stare kartice sa magnetskom vrpcom. 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 iskaznica, 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.

6. Reference

- Osnove o smart karticama - http://www.smartcardbasics.com/
- Karakteristike smart kartica - http://unix.be.eu.org/docs/smart-card-developer-kit/ewtoc.html
- Struktura podataka na smart kartici i njihova zaštita - http://home.hkstar.com/~alanchan/papers/smartCardSecurity/
- Public Key Infrastructure - http://www.opengroup.org/public/tech/security/pki/cki/
- PKI rizici - http://www.schneier.com/paper-pki.html
- RSA Laboratories - http://www.rsasecurity.com/rsalabs/