

**UNIVERZITET UNION  
RAČUNARSKI FAKULTET**

**UPOTREBA SMART KARTICA U PROCESU  
LOGOVANJA NA WINDOWS XP SISTEME**

*DIPLOMSKI RAD*

**Mentor:**

***Prof. dr Stevan Milinković***

**Student:**

***Petar Bojović***

BEOGRAD, 2007.

# SADRŽAJ

❖	<b>Uvod – predstavljanje problema</b>	<b>3</b>
❖	<b>Principi zaštite</b>	<b>4</b>
	➤ Tehnologija digitalnog potpisa	4
	➤ Zaštita tajnosti podataka	8
	➤ Infrastruktura sistema sa javnim ključevima (PKI)	12
❖	<b>Smart kartice</b>	<b>17</b>
❖	<b>Microsoft Windows okruženje</b>	<b>22</b>
❖	<b>Praktična realizacija logovanja putem smart kartica na Windows XP operativne sisteme</b>	<b>28</b>
❖	<b>Zaključak</b>	<b>36</b>
❖	<b>Literatura</b>	<b>38</b>

## Uvod – predstavljanje problema

Tempo kojim se razvijala računarska i telekomunikaciona tehnologija, praćen je tempom rasta broja korisnika tih tehnologija. Personalni računari su danas deo svakodnevnice. Znanje rada na računaru se podrazumeva kao deo pismenosti. Korisnicima su, u manjoj ili većoj meri, poznate pogodnosti koje je sa sobom doneo internet. Ovim spojem računarstva i telekomunikacija napravljen je sistem koji nudi višestruke pogodnosti uz mnogo niže cene u odnosu na tradicionalni način poslovanja.

Upravo, sve ovo je doprinelo da broj ljudi koji koristi računar postane neizbrojiv. Među korisnicima računara postoje razlike u znanju i primeni određenih oblasti iz računarstva. Iz tog razloga uvedena je korisnička klasifikacija.

Administratori su korisnici, koja imaju maksimalna prava na dodeljenu oblast. Njihovo pravo i obaveza je da osposobe i održavaju servis u svojoj oblasti. Standardnim korisnicima sa klasičnim znanjem i potrebama, dodeljuju se prava standardnih korisnika. Oni ne mogu da utiču na rad servisa već samo da ga koriste.

Tehnologija kojom se nekom korisniku dodeljuju prava, naziva se autorizacija. Međutim, pre nego što nekom korisniku dodelimo prava, moramo da ga identifikujemo. To je tehnologija autentifikacije.

Autentifikacija predstavlja jedan od ključnih elemenata u polju bezbedosti računarskih sistema. Klasičan način autentifikacije se vrši upotrebom korisničkog imena i šifre. Poznavanjem ta dva parametra, vi dokazujete sistemu da ste onaj koji tvrdite da jeste. Korisničko ime je javna stvar. Najčešće je generisano od strane administratora i lako se saznaje. Korisničku šifru postavlja sam korisnik. Ona treba da je tajna, tj. da samo on zna kako glasi.

Problem u bezbednosti sa ovim načinom autentifikacije je u tome što korisnici uglavnom biraju šifre koji su im lake za pamćenje, pa samim tim i lake za pogađanje. To su najčešće datum rođenja, ime partnera, adresa, nadimak, ime kućnog ljubimca i sl. Tu je i drugi problem, šifru treba ukucati kada je sistem traži. To znači da neko može da vidi šta ste otkucali za šifru. Sami možete da pretpostavite koliki je ovo problem, pogotovu ako za računarom imamo manje iskusnog korisnika, tj. onog koji sporo kuca. Treći problem predstavljaju virusi, softverske napasti, koji beleže sve što ste otkucali na tastaturi i šalju napadaču.

Ovakav proces logovanja je zadovoljavajući tamo gde je potreban nizak ili srednji nivo sigurnosti, ali tamo gde se govori o sigurnoj računarskoj mreži i sigurnim sistemima, svakako nije. Ako neko zloupotrebi tuđi identitet, poznavajući njegov korisnički nalog i šifru, ne postoji način da sistem ustanovi da se radi o zloupotrebi.

U okruženjima gde se zahteva visoka sigurnost primenjuju se drugačiji sistemi za autentifikaciju. U ovom diplomskom radu ću prezentovati i objasniti princip rada jednog bezbednijeg sistema autentifikacije.

## Principi zaštite

Donošenjem odluka vezanih za politiku autentifikacije i autorizacije se svakako podiže nivo sigurnosti sistema. Potrebno je implementirati mehanizme zaštite. U procesima zaštite, treba razviti sistem od poverenja. To je sistem kome se veruje u svakom trenutku, koji ima definisane politike upotrebe i politiku u slučaju zloupotrebe.

Najvažniji principi zaštite vezani za postavljanje sistema od poverenja su: tehnologija digitalnog potpisa, tehnologija zaštite tajnosti podataka, PKI infrastruktura.

### Tehnologija digitalnog potpisa

Digitalni potpis je tehnologija kojom se proverava autentičnost neke poruke, tj. znamo da je poruku poslao pošiljalac za koga znamo ko je, vrši se povera integriteta poruke, tj. poruka je ne promenjena stigla do odredišta. Ovom tehnologijom je obezbeđena i neporecivost, tj. postoji dokaz da je poruka primljena od poznatog pošaljioca.

Digitalni potpis koristi kombinaciju asimetričnih šifarskih algoritama i algoritama za heširanje.

#### Asimetrični šifarski algoritam

Poznatiji je pod nazivom šifarski sistem sa javnim ključem. To je algoritam kojim se generišu parovi ključeva. Jedan od ključeva je tajni (privatni), a drugi javni. Javni ključ je nasumično generisan broj specificirane veličine, najčešće 1024 bita. Tajni ključ se skladišti na sigurno mesto, van domašaja drugih korisnika. Sigurnost ovog sistema zavisi od kvaliteta čuvanja tajnog ključa. Javni ključ se objavljuje drugim korisnicima.

Tajni ključ se generiše tako da se zadovolji sledeći uslov :

- Poruka šifrovana javnim ključem se može dešifrovati samo tajnim ključem
- Poruka šifrovana tajnim ključem se može dešifrovati samo javnim ključem

Korisnik koji ima tajni ključ, relativno lako može izgenerisati odgovarajući javni ključ. Međutim, onaj koji ima samo javni ključ, ne sme nikako da ima mogućnost da izgeneriše tajni ključ.

Najpoznatiji algoritam za asimetrično šifriranje je Rivest-Shamir-Adleman (RSA) algoritam. Ovaj algoritam u potpunosti zadovoljava zadate uslove za asimetrično šifriranje.

Generisanje para ključeva se svodi na izbor dva prosta broja  $(p, q)$ , za koje je preporučljivo preko 200 cifara. Zatim se izračunava broj  $n = p * q$ . Posle toga se izračunava red te grupe  $\phi(n) = \phi(p * q) = (p - 1) * (q - 1)$ .

Potom se izabere broj  $e$  tako da je  $1 \leq e < \phi(n)$ , pri tom mora da važi da je  $e$  uzajamno prost sa redom, tj.  $NZD(e, \phi(N)) = 1$

Pomoću Euklidovog algoritma izračunava se  $d$ , inverzni broj broju  $e$  po modulu  $n$ .

Euklidova formula :  $e * d \equiv 1 \pmod{n}$  gde je 1 po modulu  $n$  pri čemu se za  $d$  uzima broj koji zadovoljava  $1 \leq d < \phi(n)$  .

Javni ključ predstavljaju brojevi  $n, e$  . Dok je privatni ključ brojevi  $n, d$ .

Kod RSA šifrovanje i dešifrovanje je maksimalno pojednostavljeno kako bi imao široku implementaciju. Šifrovanje javnim ključem se vrši jednostavnim računom:

$C \equiv M^e$  po modulu  $n$ . Gde je  $C$  šifrovana poruka, a  $M$  poruka u otvorenom formatu. Dešifrovanje je identičan inverzni proces :

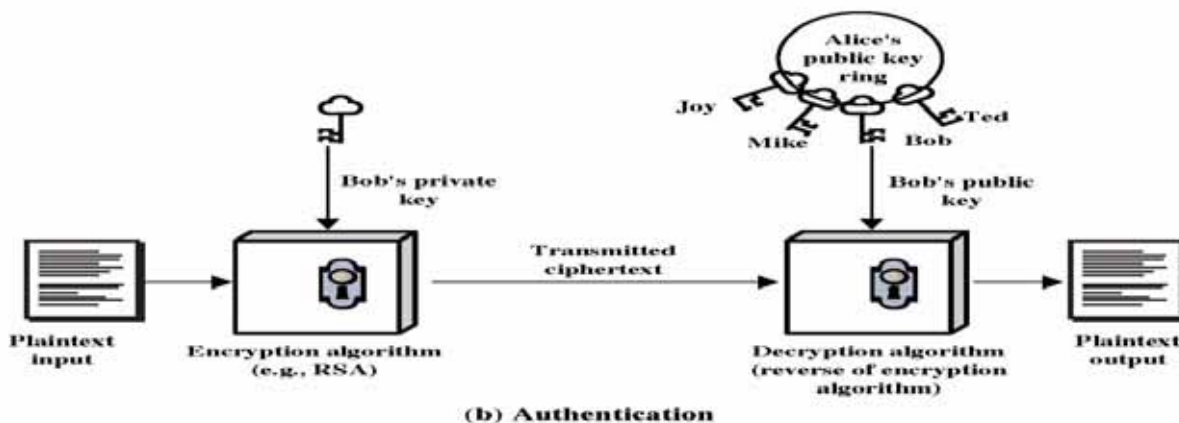
$M \equiv C^d$  po modulu  $n$ .

Pored RSA za digitalni potpis se mogu koristiti i algoritmi DSA (Digital Signature Algorithm), i ECDSA (Elliptic Curve DSA).

Asimetrični šifarski algoritmi obezbeđuju primenu najvažnijih principa zaštite :

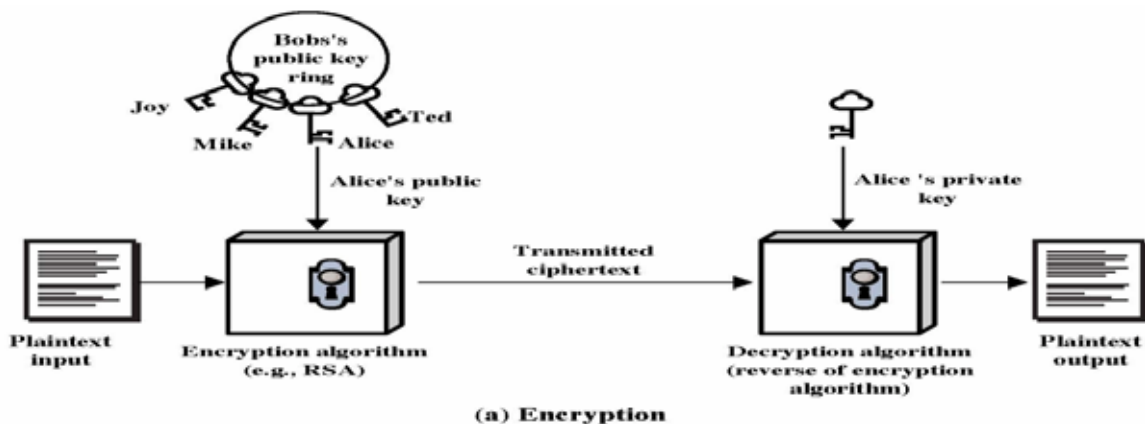
Korisnici A i B imaju generisane parove ključeva i međusobno su razmenili javne ključeve.

- Autentičnost – korisnik B kada primi poruku šifrovanu tajnim ključem korisnika A, ako uspe da je dešifruje javnim ključem korisnika A, znači da imamo potvrdu identiteta.



### *Autentifikacija upotrebom asimetričnog šifarskog sistema*

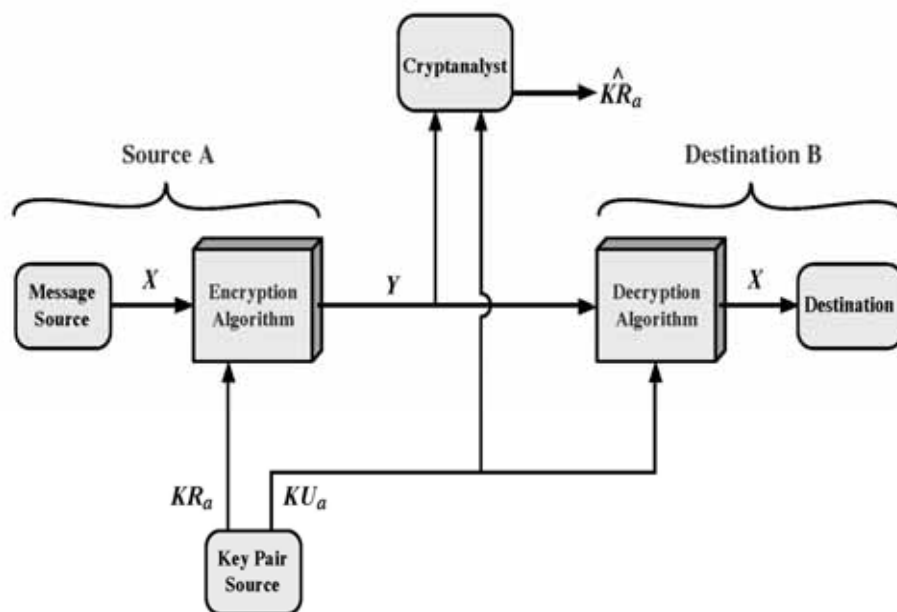
- Neporecivost – ako korisnik B uspe da dešifruje poruku javnim ključem korisnika A, znači nesumnjivo, poruka je šifrovana tajnim ključem korisnika A.
- Tajnost (Enkripcija) – korisnik A šifrjuje poruku javnim ključem korisnika B i takvu mu je šalje. Samo korisnik B može da dešifruje poruku svojim privatnim ključem. Presretač neće imati koristi.



### Zaštita tajnosti podataka upotrebom asimetričnog šifraskog sistema

Sledeći crtež predstavlja skicu gde napadač može da prisluškuje. Šta on može da sazna? Prisluškujući javnu liniju kojom komuniciraju strana A i B, sve što može da sazna jesu javni ključevi osobe A i B, kao i poruke koje se prenose u šifrovanom formatu. Da bi ih dešifrovao treba mi tajni ključ koji nikad ne napušta matični računar.

Kako se preko javnog ključa ne može generisati tajni, sigurnost ovog sistema se svodi na sigurnost skladištenja i upotrebe tajnog ključa.



### Upotreba asimetričnog šifarskog sistema

#### Algoritmi za heširanje

Sistem javnih ključeva je veoma spor da bi se samo on koristio za digitalni potpis. Ponekad sadržaj potpisa može biti iste veličine kao i sama poruka, pa čak i veća. Kako bi se rešili ovi problemi koriste se heš funkcije.

Heš funkcija ima tu osobinu da napravi otisak fiksne veličine analizirajući poruku ma koliko ona bila velika. Poruka koja se prenosi najčešće je velika i do nekoliko MB, dok otisak te poruke stane u 128 ili 160 bita. Heš funkcija se zove još i jednosmerna heš funkcija, jer jednom kreiran otisak se ne može vratiti u poruku.

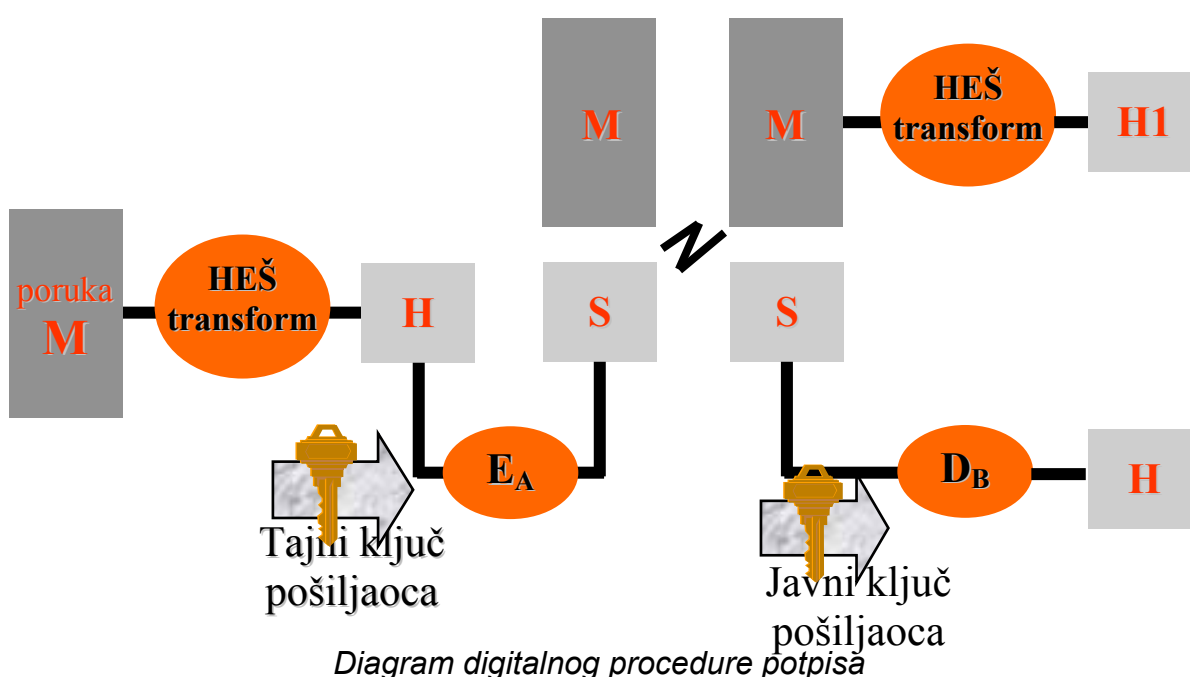
Najčešće se koriste algoritmi za heširanje MD5 (Message Digest) i SHA1 (Secure Hash Algorithm). MD5 pravi heš od 128 bita, dok SHA1 od 160 bita.

Funkcija za heširanje se svodi na odvajanje poruke na blokove od po 512 bita. Nad tim blokovima se vrše određene aritmetičke operacije kroz nekoliko faza i po više puta. Korišćenjem kompleksnih aritmetičkih operacija i višestrukim ponavljanjem se dobija efekat takav da ako se promeni samo 1 bit ceo otisak će biti potpuno drugačiji.

Heširanjem dobijamo još jednu veoma bitnu stavku bezbednosti.

- Integritet – korisnik A izračunava heš vrednost svoje poruke i šalje je zajedno sa porukom. Korisnik B kada primi poruku, izračuna heš vrednost te poruke i uporedi je sa poslatom. Ako su iste, poruka je stigla ne promenjena.

## Digitalni potpis



Digitalno potpisivanje se vrši na sledeći način :

1. Generišu se parovi ključeva asimetričnim šifarskim sistemom i pošalje se javni ključ odredišnom korisniku.
2. M – poruka koja treba da se digitalno potpiše se provlači kroz heš transformaciju nakon čega dobijamo heš vrednost H.
3. Heš vrednost šifrujemo tajnim ključem i dobijamo potpis S
4. Šaljemo poruku i digitalni potpis odredišnom korisniku
5. Primalac odvaja poruku i izvršava heš transformaciju nakon čega dobija H1
6. Dešifrira potpis javnim ključem pošiljaoca čime dobija poslat heš H.
7. Upoređuje dešifrovan i izračunat heš H i H1, ako su identični poruka je ne promenjena.

Digitalni potpis obezbeđuje sledeće :

- Autentifikaciju – javnim ključem pošiljaoca smo dešifrovali potpis, znači znam ko je pošiljaoc.

- Neporecivost – uspeo sam da dešifrujem potpis javnim ključem pošiljaoca, siguran sam da je on to poslao.
- Integritet – heš vrednost koju sam dobio dešifrovanjem je identična sa onom koju sam izračunao, poruka je ne menjana.

## Zaštita tajnosti podataka

Zaštita tajnosti ili privatnost podataka se najefikasnije postiže primenom digitalne envelope. Digitalna envelope je tehnologija koja koristi hibrid asimetričnog i simetričnog šifarskog sistema. Asimetrični šifarski sistem je veoma spor ako bi se koristio u svrhu zaštite podataka. On zahteva da se nad velikom količinom podataka vrše aritmetičke operacije sa velikim ključevima, obično 1024 bita.

### Simetrični šifarski sistem

Ovaj šifarski sistem se deli po celinama koje se šifriraju, pa tako postoje :

- Blok šifarski algoritmi
- Sekvencijalni algoritmi

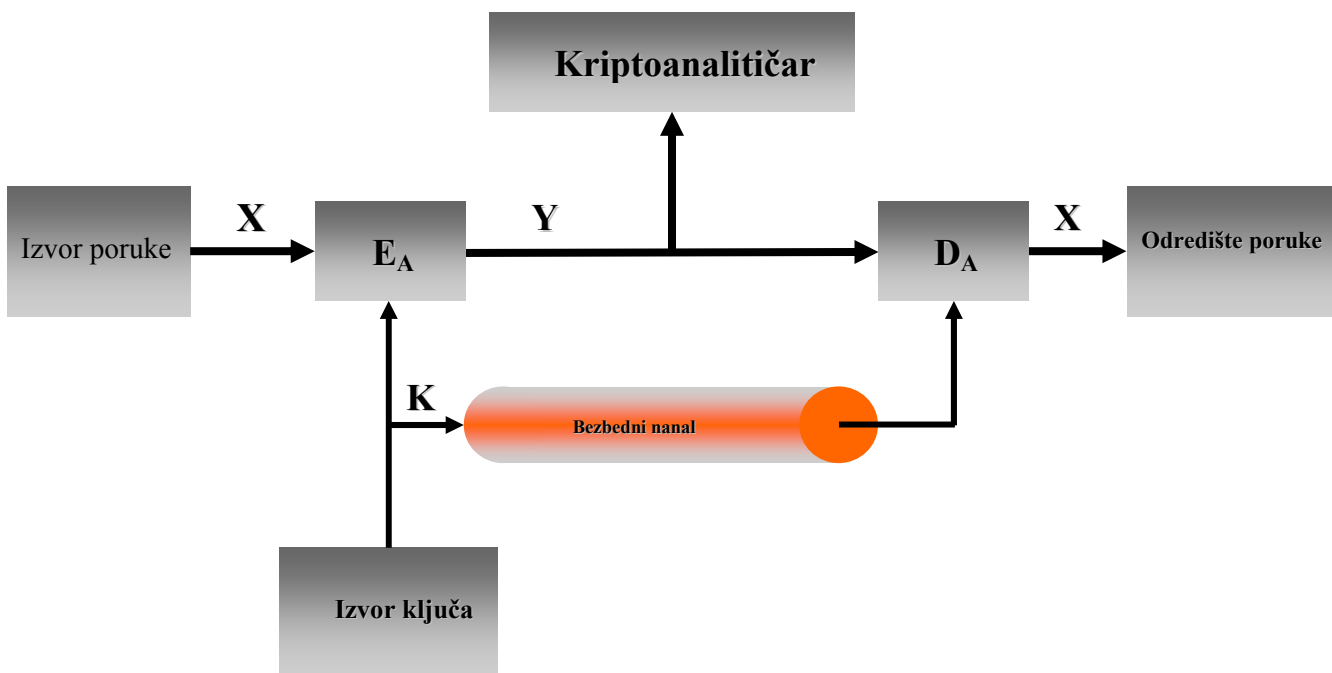
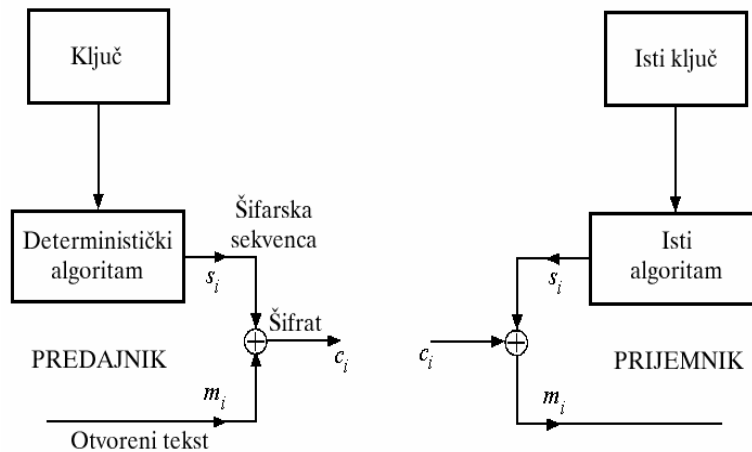


Diagram simetričnog šifarskog sistema

Kod simetričnog šifrovanja generiše se samo jedan ključ i to primenom nasumičnih metoda generisanja brojeva. Ključ se posle mora prodistribuirati svim stranama u komunikaciji i to sigurnim putem.

Istim ključem se vrši i šifrovanje i dešifrovanje.

Sekvencijalni šifarski sistem koristi simetričan ključ za generisanje pseudoslučajnih nizova koji se dalje aritmetičkom operacijom sabiranja po modulu 2, sabira sa originalnom porukom i dobija šifrovana poruka. Ista procedura se obavi i za dešifrovanje, pošto je operacija sabiranja po modulu 2 komplementarna.



### *Sekvencijalni asminterični algoritam*

Primer sekvencijalnog simetričnog algoritma je RC4.

Blok šifarski simetrični algoritmi su oni algoritmi gde se poruka šifrira u blokovima od 2 ili više elemenata. Kod ovog algoritma način šifrovanja svakog simbola zavisi od načina šifrovanja susednih. Jedna poruka šifrovana istim ključem uvek daje isti šifrat.

Algoritam za simetrično šifriranje po blokovima sastoji se od sledećih posupaka:

- Inicijalna transformacija
- Jedna kriptografski slaba funkcija ponavljanja  $r$  puta ("rundi")
- Finalna transformacija
- Algoritam za ekspanziju ključa

Primer blok šifarskih algoritama su : LUCIFER, DES, FEAL, IDEA, RC5, SKIPJACK, BLOWFISH, TWOFISH, AES.

Objasnićemo tehnologiju rada AES (Rijndael) algoritma. Ovaj algoritam predstavlja najbolju zamenu za najpopularniji DES algoritam koji je pokazao prilično slabosti razvitkom novih superbrzih računara.

### AES (Advanced Encryption Standard)

Konačna verzija AES algoritma je izabrana između 5 kandidata. AES je blok šifarski algoritam sa promenljivom dužinom bloka i promenljivom dužinom ključa. Dužine mogu biti 128, 192, 256 bita.

Osnovni element ovog algoritma je matrica Stanja koja ima 4 vrste i  $N_b$  kolona, gde je  $N_b$  dužina bloka podeljena na 32.

Ključ je takođe matrica 4 puta  $N_k$ , gde je  $N_k$  dužina bloka podeljena sa 32. Broj rundi zavisi od veličina bloka i kreće se između 10 i 14.

U okviru jedne runde prolazi se kroz sledeće transformacije :

- Nelinearna substitucija bajtova
- Ciklični pomeraj vrsta matrica
- Množenje kolona matrice Stanja fiksnim polinomom po modulu
- Sabiranjem ključa runde sa matricom Stanja

Algoritam dešifrovanja je veoma sličan algoritmu šifrovanja samo što se se u poslednjoj rundi ne vrši množenje kolona matrice Stanja fiksnim polinomom.

Nelinearna substitucija vrši transformaciju nad svim bitovima na osnovu tablice substitucije S-box.

Transformacija cikličkog pomeranja pomera vrste matrice Stanja na različite načine. Pomeranje se vrši tako da se kolona  $i$  pomera za  $C$  mesta, gde  $C$  zavisi od  $N_b$ ,  $i$  je između 0 i 3 a  $C$  između 1 i 4.

U transformaciji množenja kolona matrica Stanja se množi sa polinomom

$$3X^3 + X^2 + X + 2 \quad \text{po modulu} \quad X^4 + 1$$

U transformaciji sabiranjem ključa, ključ se sabira po modulu 2 sa svakim bitom. Dužina ključa runde je  $N_b$ . Ovaj ključ se dobija od šifarskog ključa pomoću posebnog algoritma (Key Schedule Algorithm).

Algoritam Key Schedule Algorithm se sastoji od dve komponente :

- Ekspanzija ključa
- Izbor ključa runde

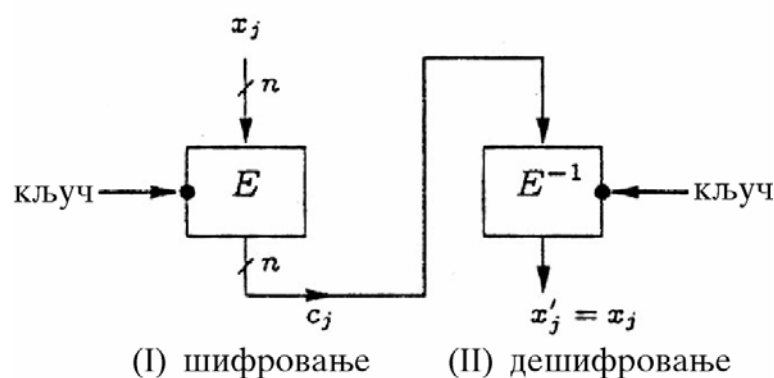
Ekspanzija je proširivanje ključa na veću veličinu, gde zavisi da li je  $N_k < 6$  ili  $N_k > 6$ .

Algoritam za izbor ključa koriguje 6 nizova po 4 bajta za svaku rundu, prvih 6 za prvu rundu, drugih 6 za drugu, i td.

Za razliku od DES-a slabi i delimično slabi ključevi ne mogu da se pojave kod AES-a. Ovaj šifarski algoritam otporan je na linearnu i diferencijalnu kriptanalizu, kao i na neke druge objavljene napade na blok šifarske algoritme.

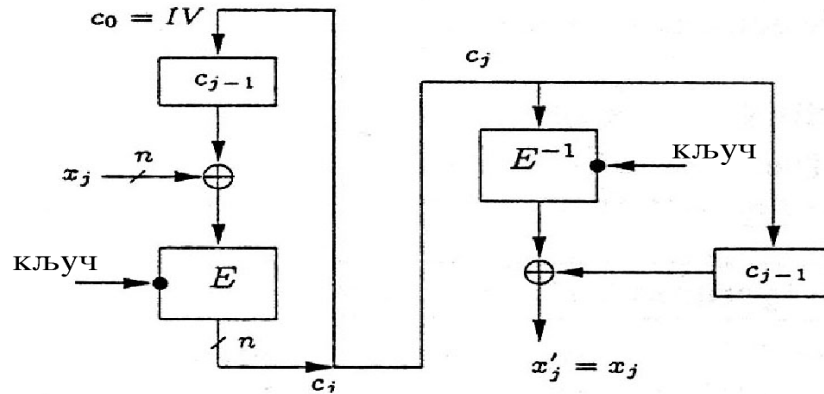
Načini rada blok šifarskih algoritama :

- Electronic Codebook, ECB



Šifrovanje se vrši direktno na blok primenom simetričnog ključa, dešifrovanje je inverzna operacija koja se vrši direktno na šifriranu poruku uz simetrični ključ.

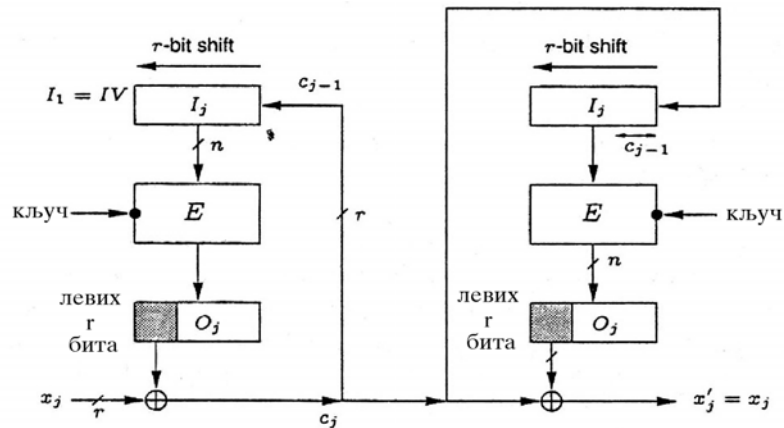
- Cipher Block Chaining, CBC



(I) шифровање (II) дешифровање

Šifrovanje se vrši na blok otvorenog teksta koji se prethodno sabere po modulu 2 sa prethodnim stanjem bloka šifrata. U prvom momentu se koristi inicijalizacioni vektor. Dešifrovanje je isto samo inverznom metodom.

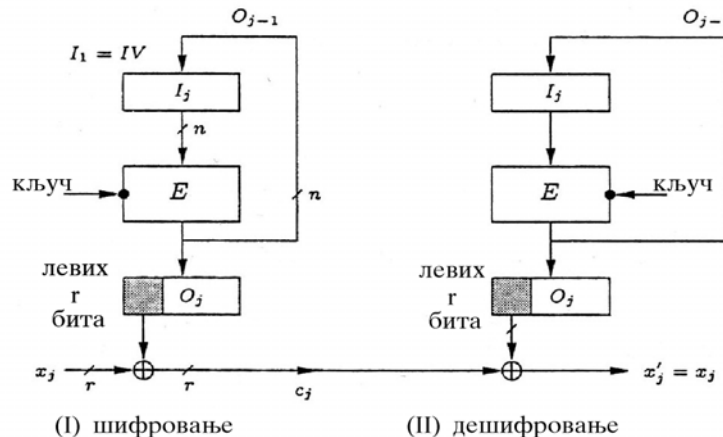
- Cipher Feedback, CFB



(I) шифровање (II) дешифровање

Šifrovanje se vrši tako što kao poruka u algoritam ulazi blok prethodnog šifrata uz simetrični ključ. Tako dobijeni šifrat se sabira po modulu 2 sa originalnom porukom i šalje. Dešifrovanje je identičan inverzni proces. Koristi se inicijalizacioni vektor.

- Output Feedback, OFB

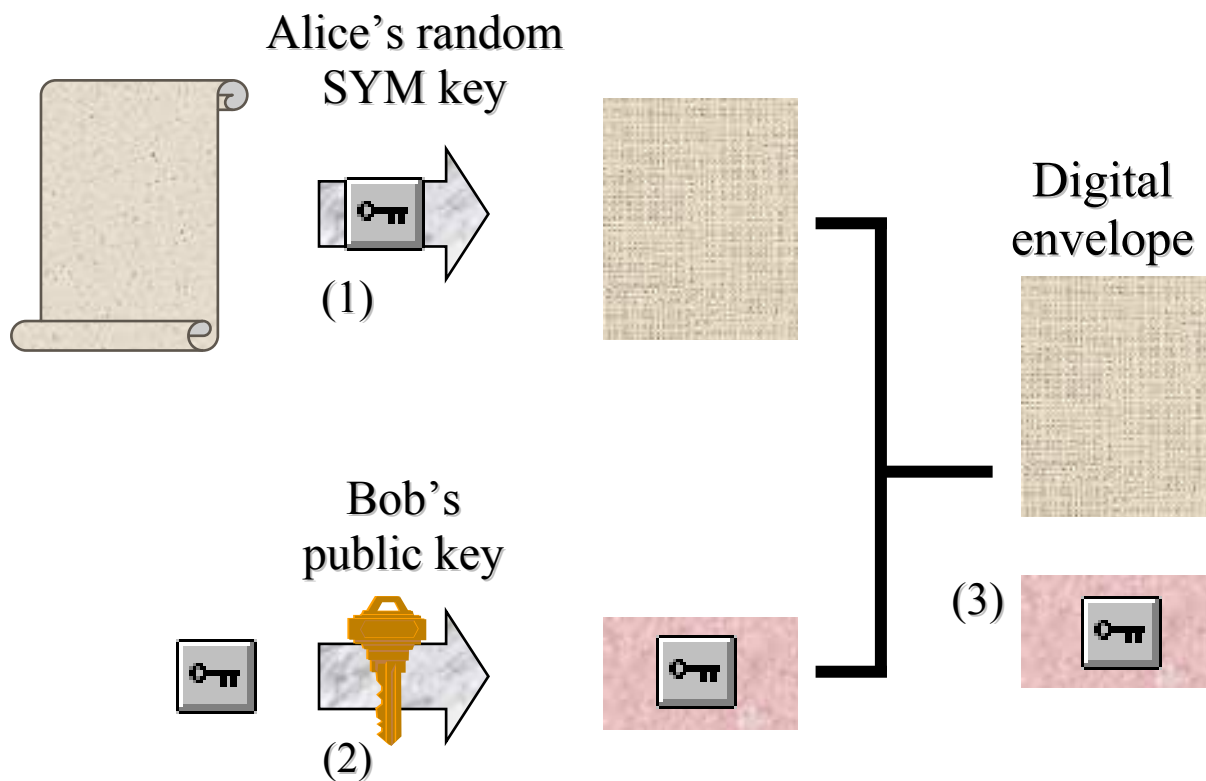


(I) шифровање (II) дешифровање

U algoritam za šifrovanje ulazi prethodni blok šifrata ali bez uticaja teksta koji se šifruje, tako dobijen šifrat je ulaz za sledeći blok i njegovih levih  $r$  bitova se sabira po modulu 2 sa tekstom. Dešifrovanje je inverzno.

## Digitalna envelope

Ovom tehnologijom obezbeđujemo efikasnu zaštitu tajnosti podataka.



### Digitalna envelope

Kako bi rešili probleme vezane za efikasnost šifriranja sa jedne strane, i prenos simetričnog ključa preko bezbenog kanala sa druge strane, napravljen je hibridni sistem.

Korisnik A želi da sačuva tajnost podataka i da pošalje poruku korisniku B, a pritom poseduje javni ključ korisnika B.

1. A generiše simterični ključ nekom slučajnom metodom. (1)
2. Simteričnim ključem šifruje poruku koju treba zaštititi
3. Taj simetičan ključ šifruje javnim ključem korisnika B (2)
4. Šalje zajedno sa šifrovanom porukom i šifrovani simterišan ključ

Svaka dalja razmena tajnih poruka se vrši šifrovanjem samo simetričnim ključem, jer smo A i B poznaju taj ključ.

### Infrastruktura sistema sa javnim ključevima (PKI)

Implementacijom tehnologije digitalnog potpisa dobijamo brojne pogodnosti u smislu potvrde identiteta, autentifikacije i integriteta. Implementacijom digitalne envelope omogućavamo zaštitu poverljivih podataka. Međutim, jedna sitnica nam je promakla. Kod asimetričnog šifrovanja, javni ključ se distribuira javnim putem. Kako da budemo sigurni da javni ključ koji smo dobili zaista pripada onome sa kim komuniciramo? Potreban nam je sistem od poverenja. Najrasprostranjeniji takav sistem je PKI sistem.

Infrastuktura sistema sa javnim ključevima omogućuje ambijent za pouzdanu primenu elektronskog poslovanja i bazira se na kombinovanoj primeni asimetričnih i simetričnih šifarskih sistema.

PKI sistem se sastoji od više komponenata, aplikacija i dokumenata koja definišu način realizacije četiri osnovne kriptografske funkcije :

- Zaštita tajnosti – simetričan šifarski sistem
- Autentičnost – asimetričan šifarski sistem
- Integritet – asimetrični šifarski sistem
- Neporecivost – asimetrični šifarski sistem

Komponente PKI sistema :

- Politika sertifikacije – CP
- Certificate Practice Statement – CPS
- Sertifikaciono telo – CA
- Registraciono telo – RA
- Sistem za distribuciju sertifikata
- PKI aplikacije

Politika sertifikacije utvrđuje osnovne principe rada sertifikacionog tela i ostalih komponenata PKI sistema.

CSP je dokument koji praktično opisuje rad sertifikacionog tela i neophodan je za rad komercijalnog CA.

Sertifikaciono telo predstavlja najvažniju komponentu i osnovu PKI sistema. Njegov zadatak je da upravlja izdavanjem digitalnih sertifikata kao i njihovim životnim ciklusom. Osnovni zadaci koje CA mora da izvršava su :

- Generiše digitalne sertifikate tako što povezuje identifikacione podatke određenog korisnika sa njegovim javnim ključem i sve to potvrđuje svojim digitalnim potpisom svih podataka u sertifikatu.
- Upravlja rokom važnosti izdatih digitalnih sertifikata
- Obezbeđuje funkciju povlačenja izdatih digitalnih sertifikata u slučajevima kada za to postoje uslovi, publikuje liste povučenih sertifikata, CRL (Certificate Revocation List) listu.

Registraciono telo obezbeđuje interfejs između korisnika i CA. RA prihvata zahteve korisnika, proverava autentičnost korisnika i prosleđuje standardni zahtev za izdavanje digitalnog sertifikata. Sigurnost autentifikacije zavisi od implementacije u RA.

Sistem za distribuciju sertifikata može da se izvede na različite načine. Sertifikat se može predati korisniku lično, ili omogućiti preko aktivnog direktorijuma.

PKI aplikacije su aplikacije za koje su implementirane 4 osnovne funkcije PKI sistema. Neke od primena su :

- Zaštita WEB transakcija
- Zaštita e-mail servisa
- VPM – Virtual Private Network
- Bezbedno upravljanje elektronskom dokumentacijom
- Kontrola radnog vremena i pristupa određenim prostorijama

- Kontrola logovanja na računarima

## CA

Sertifikaciono telo predstavlja softversko-hardversku aplikaciju koja, kao ulazni parametar, ima javni ključ, koji smešta u digitalni sertifikat zajedno sa ostalim podacima korisnika, digitalno potpisuje u cilju garancije da dati javni ključ pripada definisanom korisniku, tj. vlasniku sertifikata.

Ovim postupkom se postiže to da CA kao treća strana garantuje da je javni ključ korisnika na čije je ime izdat sertifikat. Pošto je digitalni sertifikat potpisan digitalnim potpisom CA, onda znači da je veza između naziva korisnika u sertifikatu i javnog ključa pouzdana.

Pored javnog ključa i podataka o korisniku, sertifikatu se dodaju još : datum izdavanja i rok važnosti sertifikata, ime CA koje je izdalo sertifikat, tj. sertifikat CA.

Po zahtevu, CA može da generiše parove ključeva za asimetrično šifriranje i uz sertifikat prosledi ih korisniku.

CRL lista objavljena od strane CA je digitalno potpisana potpisom CA. Svaka poruka između CA i RA mora biti digitalno potpisana. Za svaku poruku koju primi, CA verifikuje digitalni potpis.

Svi podaci koji su bitni za rad CA, kao i log fajlovi, se arhiviraju u bazi CA i svi fajlovi baze su digitalno potpisani.

CA podržava publikovanje CRL lista na različite načine. Publikovanje se može izvršiti u određenom fajlu, ili u LDAP (Aktivni direktorijum) bazi, ili na OCSP (OnLine Certificate Status Protocol) serveru.

CA treba da podržava različite hardverske elemente, npr. smart kartice, HSM module i sl. Ponekad je potrebno generisati parove ključeva na hardveru, pa onda izdvojiti javni ključ i generisati sertifikat.

CA mora da podrži različite algoritme sa simetrično i asimetrično šifrovanje. Neophodno je da podrži sledeće algoritme za digitalno potpisivanje: RSA, DSA, ECDSA.

## Digitalni sertifikati

Digitalni sertifikati predstavljaju element kojim se utvrđuje veza između identiteta subjekta i njegovog javnog ključa.

Javni ključ potpisnika mora biti na raspolaganju kako bi se uspešno verifikovao sertifikat.

Digitalni sertifikati predstavljaju elektronske ekvivalente nekoj vrsti „digitalne lične karte“ ili „digitalnog pasoša“.

Da bi se dobio digitalni sertifikat, prvo mora da se popuni zahtev i dostavi RA. Taj zahtev mora da sadrži sve zahtevane podatke koji će se pojaviti u sertifikatu, kao i javni ključ. Zahtev se zatim samo potpisuje, kako bi se sačuvao integritet.

Koriste se dva tipa zahteva za izdavanje sertifikata i to su PKCS# 10 i RFC2511. PKCS# 10 je jednostavniji i češće korišćen.

PKCS# 10 zahtev sastoji se od sledeća 4 polja :

- Broj verzije formata (od 1 do 3)
- Naziv vlasnika digitalnog sertifikata (DistinguishedName – Dname)
- Javni ključ vlasnika digitalnog sertifikata
- Atributi

U polju atributi se nalaze oni elementi koji su neophodni da se vide u digitalnom sertifikatu, npr. e-mail, telefon, username, i sl.

Polje Dname predstavlja put kroz X.500 direktorijum pa se zato može sastojati jedino od sledećih polja :

- Dvoslovni niz koji obeležava državu
- Region
- Elektronska adresa
- Firma
- Odeljenje u firmi
- Ime vlasnika sertifikata

U okviru sistema zaštite savremenih računarskih mreža, digitalni sertifikati se između ostalog, mogu primenjivati za verifikaciju digitalnog potpisa, kontrolu pristupa subjekta kriptozštićenim aplikacijama i u procedurama autentifikacije.

Sadržaj digitalnog sertifikata u skladu sa standardom X.509 je sledeći :

<b>Verzija formata sertifikata</b>
<b>Serijski broj sertifikata</b>
<b>Identifikator algoritma kojim se vrši digitalni potpis</b>
<b>Naziv CA koji je izdalo sertifikat</b>
<b>Rok važnosti sertifikata</b>
<b>Naziv vlasnika sertifikata</b>
<b>Javni ključ vlasnika sertifikata</b>
<b>Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata</b>
<b>DIGITALNI POTPIS SERTIFIKATA TAJNIM KLJUČEM SERTIFIKACIONOG TELA</b>

Digitalni sertifikat se sastoji od tri dela :

1. Podaci značajni za sam sertifikat i predstavljeni su strukturom *tbsCertificate*
2. Identifikator algoritma za potpisivanje
3. Sam potpis sertifikata

Struktura *tbsCertificate* sadrži sledeća polja:

- Verzija – oznaka verzije strukture
- Serijski broj – redni broj izdatog sertifikata

- Identifikator algoritma digitalnog potpisa, oznaka algoritma asimetričnog šifarskog sistema i identifikator heš funkcije.
- Naziv izdavača digitalnog sertifikata (Issuer) – struktura koja identifikuje sertifikaciono telo koje je generisalo dati sertifikat – Dname izdavača.
- Validnost – specificira se period unutar koje se sertifikat smatra važećim ukoliko nije opozvan. Ovo polje se sastoji od dva parametara Valid From i Valid To.
- Vlasnik sertifikata (Subject) predstavlja ime vlasnika sertifikata zapisano u obliku strukture Dname.
- Javni ključ vlasnika sertifikata i identifikacija algoritma za koji je namenjen.
- Polje dodatnih informacija (Extensions) – ekstenzije sadrže skup polja koja po potrebi mogu nositi još neke informacije osim onih u strukturi Dname. Neke od ekstenzija mogu imati atribut Critical ili Noncritical. Ukoliko aplikacija koja koristi sertifikat pronade ekstenziju označenu sa Critical a ne prepozna je, odbacuje sertifikat kao neispravan.

Prema dosadašnjim iskustvima ovakva struktura sertifikata ispunjava zahteve savremenih kriptografskih sistema zaštite. Savremeni sistemi zaštite baziraju se na primeni X.509 digitalnih sertifikata.

Ekstenzije u sertifikatu su uvedene od definisanja X.509v3 standard sertifikata. U ranijim verzijama, sve dodatne informacije su morale da se u pišu u okviru Dname strukture.

Upotreba ekstenzija čini savremene sertifikate izuzetno fleksibilnim, zato što povećavaju mogućnost proširenja PKI na nove aplikacije. Ekstenzije se koriste za dodeljivanje atributa vlasniku koji su različiti od onih unetih u okviru Dname-a.

Postoji mnogo predefinisanih ekstenzija, ali mogu se definisati i generičke ekstenzije za privatne potrebe.

Polja za ekstenzije se mogu koristiti kako bi obezbedili dodatne identifikacione parametre, autentifikacioni podaci i polja kontrole pristupa. Ekstenzije mogu da sadrže sve što korisniku može poslužiti u procesu analize sertifikata.

Standardne ekstenzije u certifikatu su:

- Identifikator ključa autoriteta (Authority Key Identifier),
- Identifikator ključa subjekta (Subject Key Identifier),
- Upotreba ključa (Key Usage),
- Period korišćenja privatnog ključa (Private Key Usage Period),
- Politike sertifikacije (Certificate Policies),
- Mapiranje politike (Policy Mappings),
- Alternativno ime subjekta (Subject Alternative Name),
- Alternativno ime izdavača sertifikata (Issuer Alternative Name),
- Direktorijumski atributi subjekta (Subject Directory Attributes),
- Osnovna ograničenja (Basic Constraints),
- Ograničenja vezana za ime subjekta (Name Constraints),
- Ograničenja vezana za primenjenu politiku (Policy Constraints),
- Prošireno korišćenje ključa (Extended Key Usage),
- Distributivne tačke za listu povučenih sertifikata - CRL (Certificate Revocation List) Distribution Points.

Najčešće ekstenzije prisutne u v3 verziji digitalnih sertifikata su:

- Osnovna ograničenja (Basic Constraints). Preko navedene ekstenzije se specificira da li vlasnik datog sertifikata može da generiše digitalne sertifikate za ostale korisnike (Subject Type=CA) ili ne (Subject Type=End Entity).
- Specifikacija primene ključa (Key Usage). Data ekstenzija određuje namenu ključa asimetričnog algoritma specificiranog u digitalnom sertifikatu. Moguće je definisati sledeće primene ključa:
  - kreiranje digitalnog potpisa poruka (Digital Signature),
  - dešifrovanje poruka čime se može ostvariti funkcija neporecivosti (Non-Repudiation),
  - šifrovanje simetričnog ključa (KeyEncipherment) koje se primenjuje u procesu kreiranja sesijskog ključa ili digitalne envelope,
  - šifrovanje poruka (DataEncipherment),
  - kreiranje digitalnog potpisa sertifikata (Certificate Signing).

Dodatna specifikacija primene ključa (Enanced Key Usage). Data ekstenzija definiše dodatnu namenu ključa asimetričnog algoritma specificiranog u digitalnom sertifikatu.

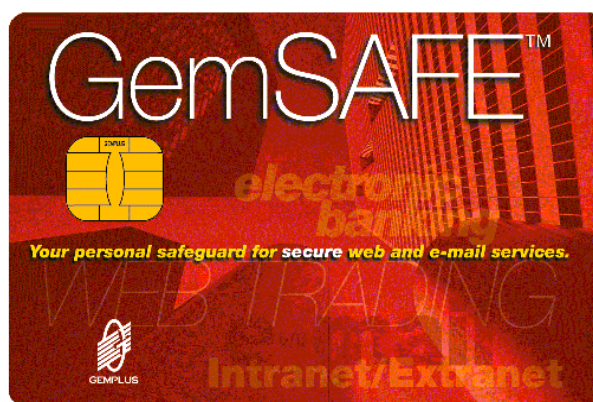
Moguće je definisati sledeća proširenja primene ključa:

- digitalno potpisivanje izvršnog programa (Code Signing),
- digitalno potpisivanje poruka koje se prenose posredstvom elektronske pošte (Secure email),
- autentikacija servera prilikom kreiranja kriptografskog tunela sa klijentskim računom (Server Authentication),
- autentikacija klijenta prilikom kreiranja kriptografskog tunela sa serverskim računom (Client Authentication).

Politika primene digitalnog sertifikata (Certificate Policy). Data ekstenzija pblži definiše politiku i način primene datog digitalnog cerifikata. Svaka politika primene sertifikata je predstavljena sa:

- oznakom date politike (Policy Qualified ID),
- vrednošću koja opisuje način primene sertifikata u skladu sa specificiranom politikom (Qualified).

## Smart kartice



*Smart Kartica*

Smart kartice nude značajno viši nivo bezbednosti u odnosu na samo softverska rešenja za realizaciju funkcija: bilateralne autentikacije, digitalnog potpisa, bezbednog čuvanja tajnih podataka i sistemske administracije.

S obzirom da poseduju memoriju koja je mikroprocesorski zaštićena od neautorizovanog pristupa, skladištenje osetljivih informacija kao što su kriptografski ključevi, digitalni sertifikati, lozinke i druge forme ličnih informacija na smart karticama je značajno bezbednije nego na drugim medijumima (kao na primer disketama i mini CD).

Smart kartice takođe mogu realizovati asimetrične kriptografske algoritme za primenu digitalnog potpisa, kao i javne simetrične algoritme, bez ikakvog prikazivanja ključeva u okviru PC računarskog sistema.

U savremenim računarskim mrežama predlažu se smart kartice za generisanje digitalnog potpisa, generisanje asimetričnih ključeva, za bezbednu identifikaciju subjekata i kao portabilni nosioci javnih i tajnih kriptografskih parametara.

Kartica sadrži javno dostupni deo i PIN (Personal Identification Number) kodom zaštićeni deo memorije u kojima se smeštaju kriptografski parametri.

Postoji nekoliko vrsta smart kartica:

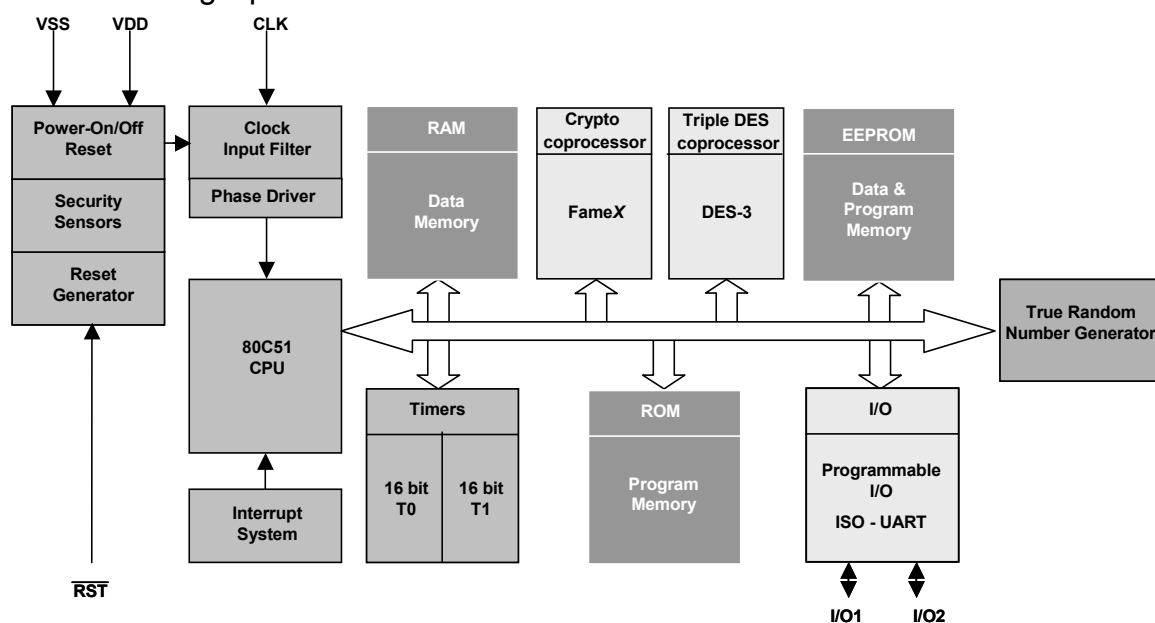
- Memorijske kartice,
- Mikroprocesorske smart kartice sa korišćenjem PIN koda za pristup,
- Mikroprocesorske smart kartice sa PKI mogućnostima (generisanje i čuvanje asimetričnih ključeva, digitalno potpisivanje).

Što se tiče tipa mikroprocesora implementiranih na smart karticama, pretežno su to 8-bitni mikrokontroleri, i to najčešće iz klase Intel 80C51 mikrokontrolera.

U poslednje vreme se pojavljuju i smart kartice bazirane na 16-bitnim i 32-bitnim mikrokontrolerima.

Ovi čipovi po pravilu poseduju dodatne kripto-koprocitore za realizaciju asimetričnih kriptografskih algoritama – digitalno potpisivanje (na primer FameX kripto čip, kao najčešće korišćeni kriptokontroler za realizaciju asimetričnih kriptografskih algoritama u smart karticama) i za realizaciju simetričnih algoritama (DES-3 kripto-koprocisor) za realizaciju zaštićene razmene podataka (secure messaging) između smart kartice i softvera na PC računaru

Primer 8-bitnog čipa smart kartice.



Arhitektura smart kartice

Primena smart kartica u mnogome zavisi od operativnog sistema implementiranog na primenjenom čipu, kao i od eventualnih preprogramiranih aplikacija.

U odnosu na primenjene operativne sisteme, smart kartice se dele na: smart kartice sa privatnim operativnim sistemom i JAVA smart kartice.

Smart kartice sa privatnim operativnim sistemom su mnogo rasprostranjenije i njihove osnovne karakteristike su: niska cena, mogućnost rada na jednostavnijim mikroprocesorima (8-bitnim) i male mogućnosti prilagođenja (kustomizacije) implementiranih funkcija na smart kartici.

Sa druge strane, JAVA kartice nude veću mogućnost kustomizacije zahvaljujući postojanju JAVA virtualne mašine koja izvršava JAVA aplete definisane od strane korisnika na samoj kartici.

Međutim, s obzirom da su se pojavile u skorije vreme, JAVA kartice su skuplje od "običnih" kartica i bolje rade na čipovima koji se baziraju na jačim mikroprocesorima (16-bitni i 32-bitni).

U smart kartičnoj industriji postoji nekoliko grupa učesnika: proizvođači čipova, proizvođači operativnih sistema i aplikacija, proizvođači-integratori kompletne kartice (čip, plastika, implementacija čipa, ugradnja operativnog sistema) i isporučioци kompletnih sistema za masovnu produkciju i personalizaciju (vizuelnu i logičku) smart kartica.

Neke kompanije su osposobljene za realizaciju više gore pomenutih operacija, a neke su specijalizovane samo za jednu operaciju. Tako na primer, Phillips i Siemens-Infineon su tradicionalni proizvođači čipova, dok su: GemPlus, SchlumbergerSema, Oberthur, Bull, Giesecke & Devrient, Datacard, ActivCard, Orga, itd. proizvođači operativnih sistema i aplikacija za smart kartice.

Posebno su od interesa kombinovane smart kartice (kontaktne i beskontaktne – imaju kontaktni čip i beskontaktni čip sa antenom) koje mogu, pored PKI primene za kriptozštićene aplikacije (kontaktni čip), da se koriste i za kontrolu pristupa u određene prostorije u kompaniji, itd. (beskontaktni čip).

U okviru PKI sistema, smart kartice imaju sledeću funkcionalnost i obeležja:

- Generisanje ključeva na smart kartici – generisanje para ključeva asimetričnog kriptografskog algoritma, kao i zahtevanog broja simetričnih ključeva (opciono), realizuje se unutar smart kartice.
- Bezbedno čuvanje kriptografskih parametara – ključevi se bezbedno čuvaju u zaštićenom delu memorije smart kartice.
- Smart kartice su same po sebi „tamperproof“ moduli.

Smart kartica je sposobna da realizuje kriptografske funkcije na samoj kartici ali sporije nego na HSM modulima.

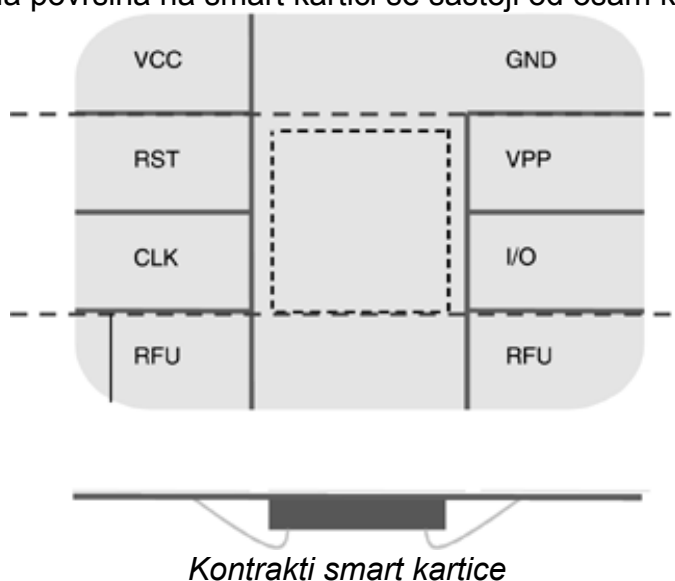
Smart kartice su mikoračunari koji sadrže više vrsta memorija. ROM memoriju u kojoj čuvaju operativni sistema, kapaciteta od 4 do 96 KB. RAM memoriju, koja se koristi za privremeno smeštanje promenljivih u toku izvršenja kriptografskih funkcija. Kapacitet ove memorije je nekoliko kilobajta. NVM memorija (Non Volatile Memory) je memorija u kojoj se sadržaj čuva i kada prestane dovod napajanja. Najčešće se kao NVM memorija koristi E2PROM memorije. Za upis podataka se garantuje tajnost čuvanja od 10 godina. Ukupan broj upisa na jednu lokaciju limitiran je i iznosi 100000. Vreme upisa je znatno duže od vremena čitanja.

Ulazno/izlazni sistem na smart karticama je namenjen za realizaciju komunikacije sa čitačem kartica (Smart Card Reader). Za komunikaciju sa čitačem zadužena je UART komponenta (Universal Asynchronous Receiver Transmitter) smart kartice koja primenom asinhronog serijskog protokola razmenjuje podatke sa

čitačem. UART komponenta smart kartice omogućava brzinu prenosa od 115 200 bita u sekundi.

Komunikacija sa PC računarom se ostvaruje preko serijskih COM ili USB portova.

- Beskontaktne smart kartice (contactless card). Komunikacija između čitača i smart kartica se obavlja preko radio talasa. Date kartice su u današnje vreme našle primenu u sistemima za kontrolu pristupa određenim prostorijama ili u javnom saobraćaju gde se mora izvršiti kontrola većeg broja ljudi u što kraćem vremenu.
- Klasične smart kartice sa kontaktnim interfejsom prema čitaču. Kontaktna površina na smart kartici se sastoji od osam kontakata.

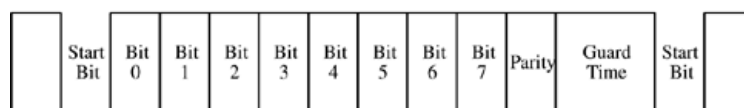


Osnovni način komunikacije između čitača smart kartica (terminal) i smart kartica je da terminal šalje komandu ka smart kartici koja je izvršava i šalje rezultat obrade ka terminalu.

Operativni sistem smart kartice je odgovoran da interpretira primljenu komandu, zada odgovarajuće upravljačke signale ka drugim uređajima na smart kartici, prihvati rezultate obrade, formira odgovor i prosleđuje ka terminalu.

Savremene smart kartice najčešće koriste dva serijska protokola za komunikaciju sa čitačem smart kartica: T0 i T1.

Protokol T0 je karakter orijentisani protokol koji u jednom paketu razmenjuje 8-bitne podatke. Provera ispravnosti korektnosti primljene poruke se ostvaruje proverom bita parnosti



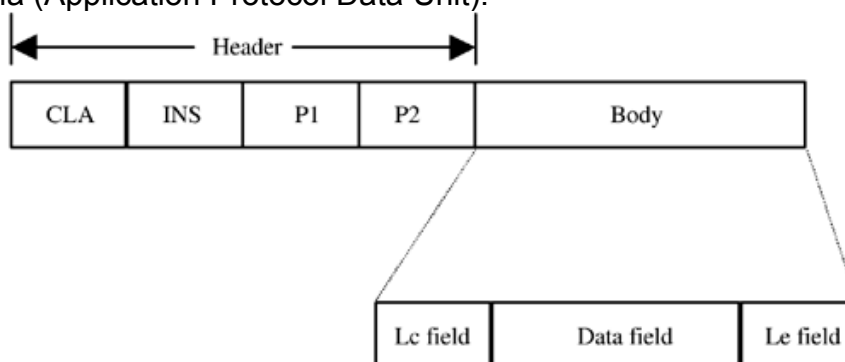
*T0 protokol*

T1 je blok orijentisani serijski protokol što označava da je najmanja jedinica prenosa blok podataka.

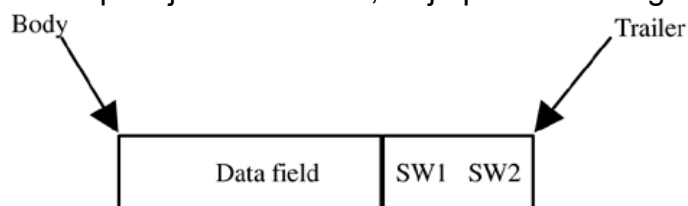
Prologue Field			Information Field	Epilogue Field
Node Address	Protocol Control Byte	Length	APDU	Error Detection
NAD	PCB	LEN	Data Length	LRC/CRC
1 byte	1 byte	1 byte	0 to 254 bytes	1 or 2 bytes

*T1 protokol*

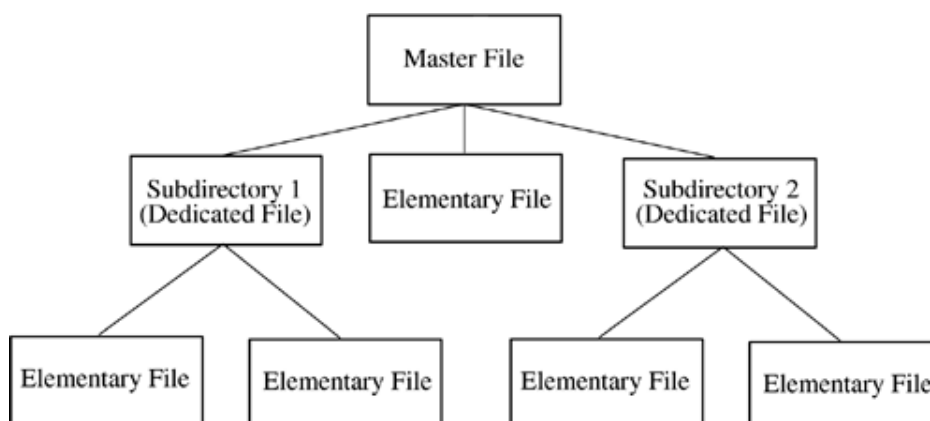
Aplikacija komunicira (zadaje komande) sa smart karticama posredstvom APDU protokola (Application Protocol Data Unit).



Smart kartica, nakon primljene komande, šalje poruku sa odgovorom.



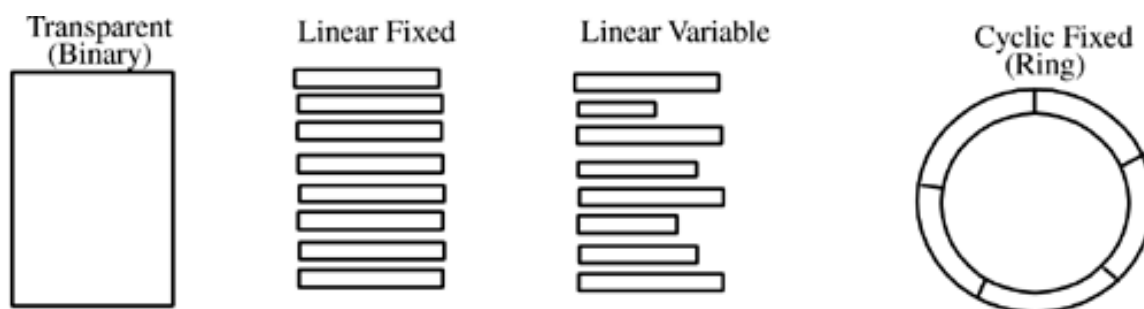
Organizacija fajlova na smart kartici je sledeća:



Četiri osnovna tipa fajlova na smart kartici su:

- binarni fajlovi (transparent file)
- linearni sa fiksnom dužinom zapisa (linear, fixed-length record file)
- linearni sa promenljivom dužinom zapisa (linear, variable-length record file)

- ciklični, sa fiksnom dužinom zapisa (cyclic, fixed-length record file)



*Tipovi fajlova (EF) na smart kartici*

Kombinacijom softvera i hardvera možemo dobiti vrhunske rezultate na polju sigurnosti. Tako recimo, ako koristimo smart kartice za generisanje parova ključeva, privatni ključ nikad ne napušta karticu i hardverski je zaštićen od bilo kakvog kopiranja. Izvozimo samo priatni ključ kako bi generisali sertifikat (predali zahtev CA), nakon čega bi i sertifikat vratili na karticu.

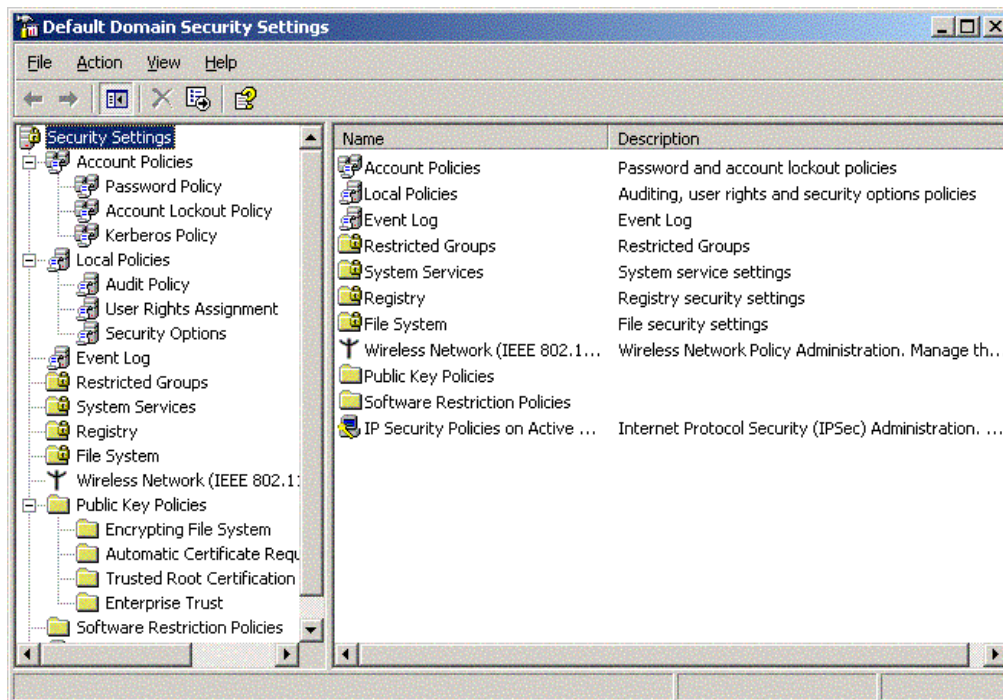
Telekom koristi smart kartice memorijskog tipa za svoje telefonske govornice. Za naše potrebe potrebna je smart kartica sa PKI mogućnostima i sa mogućnošću generisanja ključeva na kartici.

## Microsoft Windows okruženje

Microsoft je implementirao podršku za mrežni rad koristeći jedan od dva principa, princip radnih grupa – workgroup, i princip domena. Kod radnih grupa svi računari su jednaki u mreži. Svaki sistem mora zasebno da se podešava i svaki radi na svoj način. Korisnici se ručno ubacuju na svaki računar na kome je potreban određeni pristup. Koristi se isključivo korisničko ime i šifra kao način logovanja.

Domenska organizacija je potpuno suprotnog tipa. Podržana je na sistemima koji se baziraju na NT platformi. Windows XP podržava članstvo u domenu. Svaki domen ima makar jedan domen kontroler. To je server koji predstavlja centralizovano mesto za upravljanje konfiguracijama računara, korisničkim nalogima, DNS zapisima tog domena, LDAP serverom, ili kako to Microsoft naziva Aktivnim direktorijumom. Aktivni direktorijum je ukratno baza svih podataka vezana za jedan domen. Samo Windows Server operativni sistemi mogu biti domen kontroleri i formirati aktivni direktorijum.

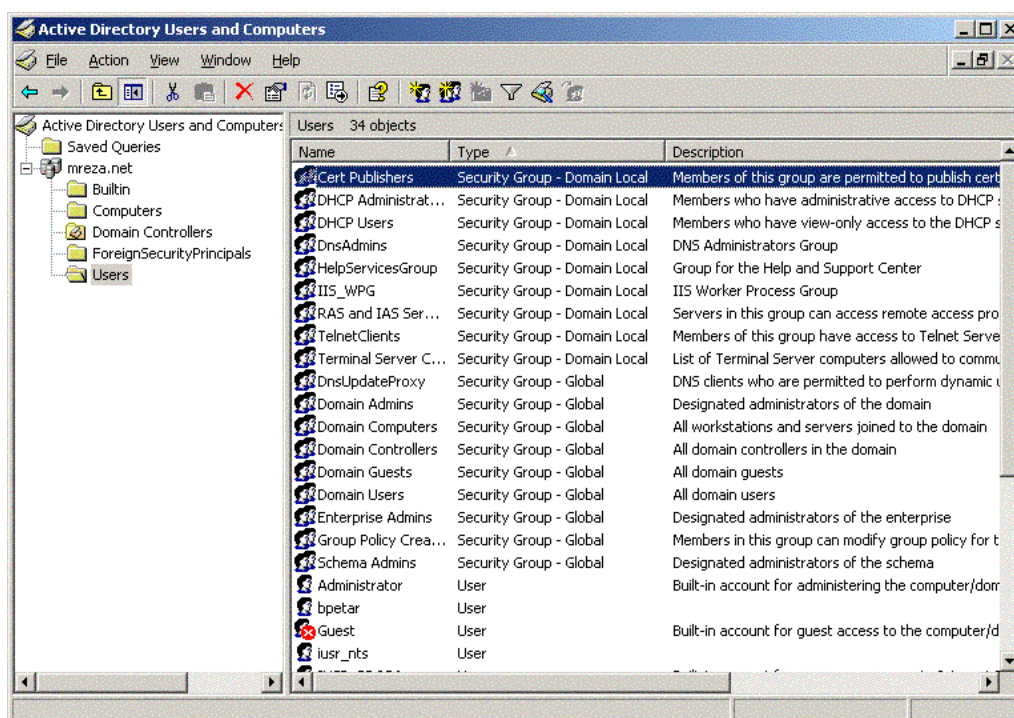
Učlanjivanjem radnih stanica, tj. Windows 2000, Windows 2003 ili Windows XP sistema na određeni domen, omogućava se logovanje određenih grupa korisnika. Aktivni direktorijum sadrži bazu korisnika koji su registrovani na domenu. Tu su raspoređeni u administrativne grupe, u zavisnosti od prava pristupa, i dodeljena su im autorizaciona prava. Svaki korisnik domena može da se uloguje na svaki računar koji je član tog domena, ukoliko politikom nije drugačije rečeno.



*Default domenska politika*

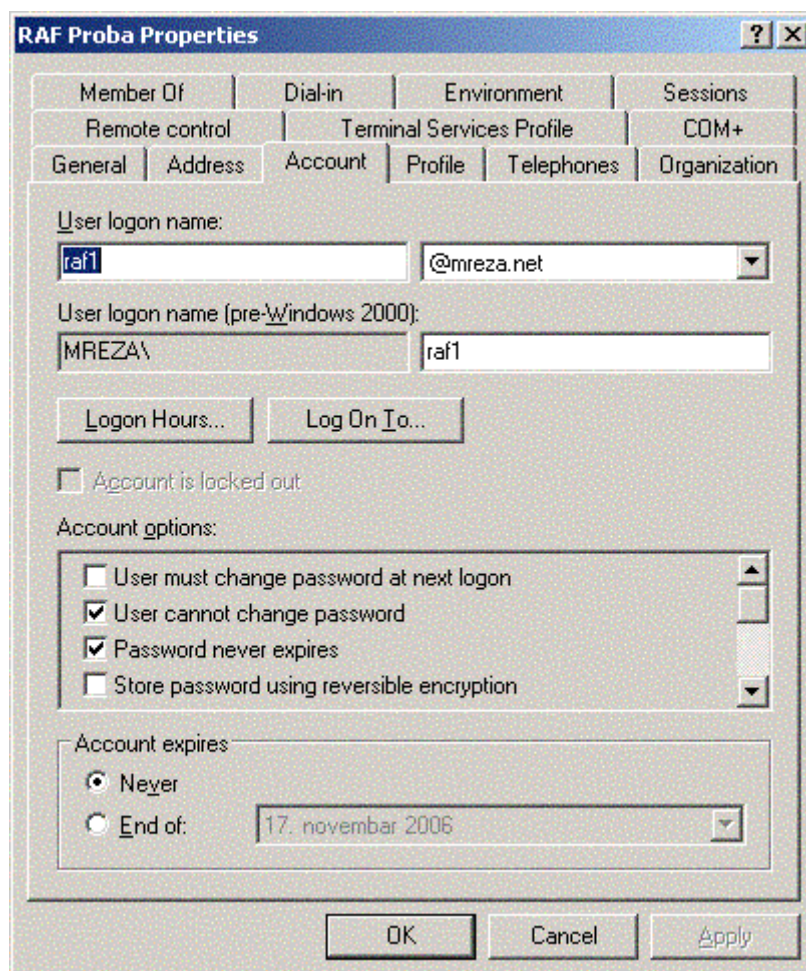
Domenskom politikom se vrši podešavanje konfiguracionih parametara sistema članova. Uvek postoje dve osnovne politike, default politika svih računara članova, i politika za domen kontrolere. Pored ovih politika možemo kreirati i posebne politike za određenu grupu računara, za one koji treba da imaju drugačije konfiguracije od ostalih.

Administracija korisnika se vrši centralno, iz konzole koja pristupa aktivnom direktorijumu. Odatle se generalno vrši menadžment članova domena, tj. objekta domena. Iz konzole se upravlja korisnicima, grupama, računarima članovima domena, domen kontrolerima, organizacionim jedinicama, štampačima i sl.



*Konzola za upravljanje objektima aktivnog direktorijuma*

Rad sa korisničkim nalogom pruža prilično mogućnosti za podešavanje ponašanja korisnika u mreži. Korisnici su uglavnom članovi više organizacionih grupa, po default-u su članovi grupe Domain Users. Grupe se dele na : Security Global – predefinisana grupa koja donosi velika autorizaciona prava za određene servise, Security Local – grupa definisana od strane administratora za potrebe definisanja različitih nivoa prava pristupa, Distribucione grupe – čiji članovi mogu biti i druge grupe.



*Konfiguracija korisnika*

Jednom korisničkom nalogu treba pridružiti njegove identifikacione osobine: ime, prezime, mail, opis, adresa, i najvažnije za domen, username. Korisničkom nalogu se može dodatno definisati gde sme da se loguje, kada sme, da li nalog automatski ističe, da li šifra automatski ističe i sl. Pod opcijom profile se vrše podešavanja vezana za njegove personalne podatke. Tako na primer, tu se može upisati putanja do roaming profila sa udaljenog servera, ili zadati automatsko mapiranje Home direktorijuma sa nekog udaljenog servera.

U polju member of se korisnik priključuje grupama, različite grupe daju različita autorizaciona prava. Korisniku se može dozvoliti upotreba i terminal prilaz određenim računarima, ili terminal serveru.

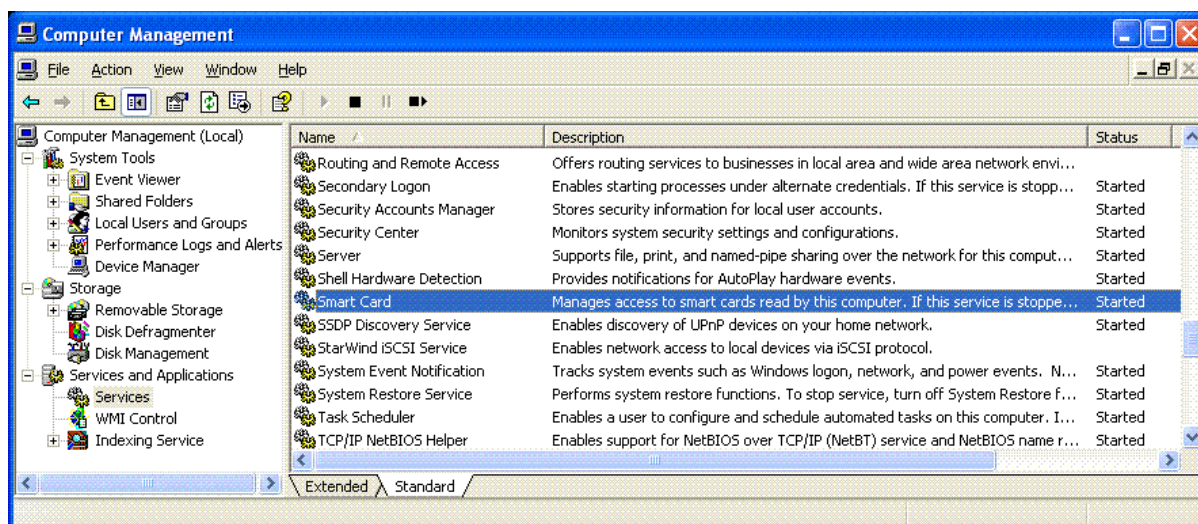
Microsoft podržava dva načina autentifikacije na NT baziranim sistemima. To su logovanje korišćenjem korisničkog imena i šifre, i logovanje putem smart kartica.

Za logovanje standardnim putem, putem korisničkog imena, potrebno je otvoriti nalog na domen kontroleru. Prilikom otvaranja naloga administrator će biti upitan za inicijalnu šifru. Nakon otvaranja naloga, može se koristiti na svim računarima u domenu, jednostavnim odnošenjem korisničkog imena i šifre u odgovarajuće polje.



*Okvir logovanja korišćenjem korisničkog imena i šifre*

Proces logovanja na računare u domenu je dosta komplikovaniji jer zahteva određene PKI funkcije i sertifikate. Naime, proces logovanja se obavlja tako što kada korisnik ubaci svoju smart karticu u čitač na računaru na kom želi da se prijavi, servis Smart Card primeti prisustvo kartice i očekuje download digitalnog sertifikata radi provere. CSP (Crypto Service Provider) je zadužen za komunikaciju sa karticom. On downloaduje digitalni sertifikat sa kartice i postavi je u private store za digitalne sertifikate.



*Smart Card servis*

Servis smart card nakon prijema sertifikata, počinje sa proverom. Prvo se proverava da li postoji sertifikat izdavača u bazi digitalnih sertifikata (storage) ili u sertifikatu pročitanoj sa kartice. Ako ne pronađe traženi sertifikat to znači da izdavač nije u bazi tj. nije izdavač kome se veruje. Proces se prekida i logovanje je neuspešno. Ako pronađe sertifikat izdavača, znači da je to izdavač kome verujemo,

možemo proveriti potpis sertifikata i ustanoviti integritet. Time što smo uspešno proverili digitalni potpis sertifikata neporecivo znamo da je taj izdavač izdao sertifikat. Nakon analize sertifikata, servis proverava CRL fajl izdavača, da bi utvrdio da li je sertifikat povučen. Ako nije povučen i još je u periodu važenja, servis nastavlja proces.

Iako sertifikat sadrži podatke o vlasniku tj. korisniku u Dname polju, servis zahteva da postoje odgovarajuće ekstenzije koje sadrže tačnu identifikaciju korisnika, kao i tačnu identifikaciju domena i domen kontrolera. Ako servis nađe odgovarajuće ekstenzije obaveštava domen kontroler i šalje Challenge random broj PKI smart kartici preko CSP-a. Komunikacija između Smart Card servisa i domen kontrolera se obavlja tajnim putem, preko envelope koju servis šalje domen kontroleru. Challenge je proces kojim servis generiše random broj i šifruje ga tajnim ključem iz sertifikata sa kartice. Tako šifrovano se šalje preko CSP-a kartici koja treba da ga dešifruje i vrati servisu. Dešifrovanje će biti uspešno samo ako postoji odgovarajući tajni ključ na kartici, što potvrđuje da je provereni sertifikat stvarno sa kartice. Servis o svakoj komunikaciji sa karticom obaveštava domen kontroler, i ako je challenge uspešan počinje proveru korisnika čije je podatke analizirao servis koristeći ekstenzije.

Ako domen kontroler ustanovi da korisnik ispunjava sve uslove za logovanje, ima sva autorizaciona prava, potvrđuje autentifikaciju i proces logovanja počinje.

Microsoft je propisao pravila koja treba ispoštovati da bi sistem prihvatio logovanje putem smart kartica. Osnovna pravila su :

- U aktivnom direktorijumu mora biti učitani i proglašeni CA izdavač sertifikata za smart card logovanje
- Domen kontroler mora da ima svoj sertifikat kako bi mogao da komunicira sa servisom sigurnim putem
- Digitalni sertifikati moraju isključivo biti u propisanom obliku
- Na smart kartici mora da postoji privatni ključ
- Kartica mora da podržava PKI funkcije

Propisan postupak pripreme sistema za upotrebu smart kartica izgleda ovako :

1. Nabaviti root sertifikat CA u Base 64 enkodovanom X.509 formatu
2. U okviru domenske politike treba ubaciti CA sertifikat u Trusted Root Certification Authorities, kako bi svi računari domena prihvatili CA kao CA od poverenja.
3. Importovati sertifikat CA u aktivni direktorijum u bazu NTAAuth što omogućava da sertifikati ovog izdavača budu razmatrani za smart card logon.
4. Napraviti sertifikat za domen kontroler, sertifikat mora biti u propisanom formatu.
5. Napraviti zahtev za CA i generisati sertifikate za smart card logon koristeći striktna pravila oblika sertifikata
6. Instalirati na radne stanice drajvere od čitanih smart kartica kao i CSP za komunikaciju sa karticom
7. Ako CSP nije prekopirao digitalni sertifikat sa kartice u Personal store korisnika, importujte sertifikat ručno.
8. Uploadujte sertifikat na smart karticu, postupak zavisi od CSP-a
9. Logujte se koristeći formiranu karticu.

Zahtevi ekstenzija za sertifikat domen kontrolera :

- Key Usage mora biti Digital Signature, Key Encipherment

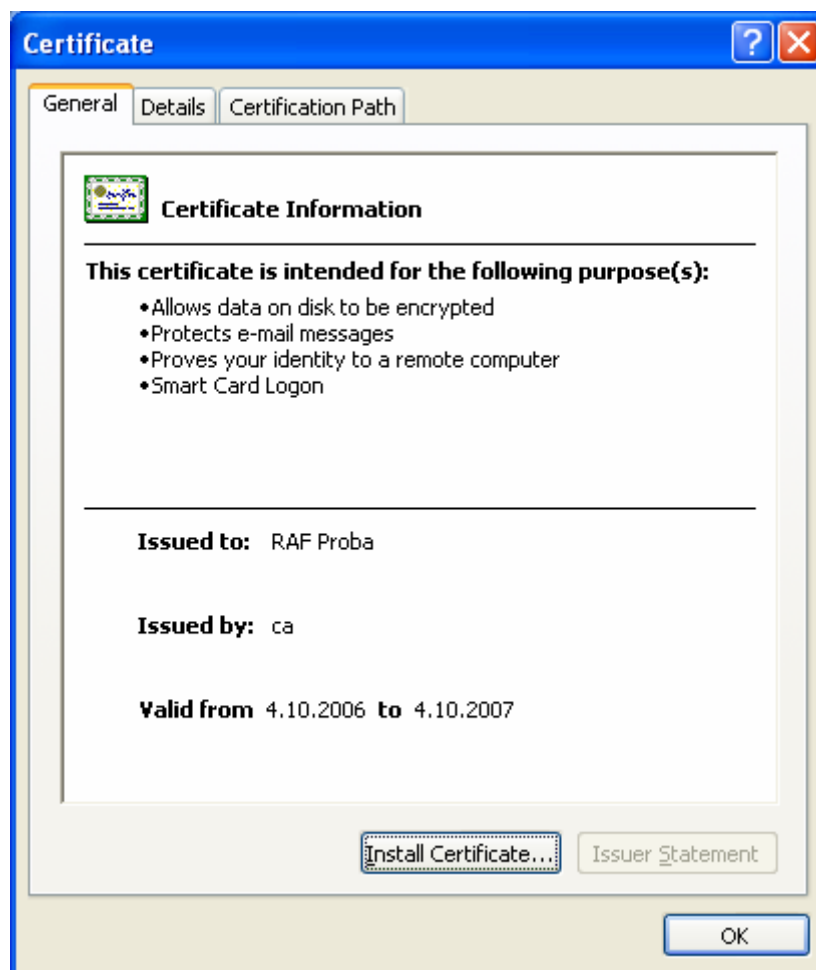
- Enhanced Key Usage mora biti
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - Server Authentication (1.3.6.1.5.5.7.3.1)
- Subject Alternative Name mora sažati globalni jedinstveni identifikator domena (GUID) kao i ime domena i to u formi npr :

Other Name: 1.3.6.1.4.1.311.25.1 = ac 4b 29 06 aa d6 5d 4f a9 9c 4c bc b0 6a 65 d9  
 DNS Name=server1.northwindtraders.com

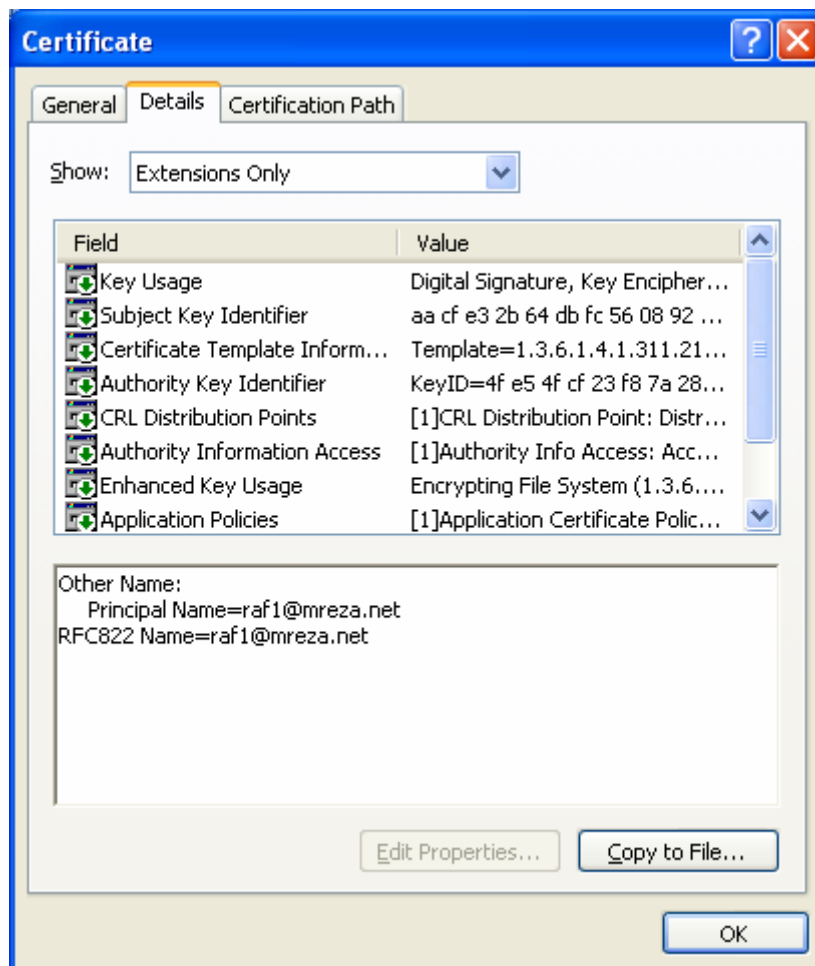
- Mora da se koristi Schannel CSP za generisanje parova ključeva

Zahtevi ekstenzija za logovanje putem smart kartica :

- RL Distribution Point (CDP) mora da ukazuje na ispravan CRL fajl, ako ne uspe da se proveri CRL logovanje neće uspeti
- Key Usage = Digital Signature
- Enhanced Key Usage =
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Subject Alternative Name = Other Name: Principal Name= (UPN), na primer: UPN=raf1@mreza.net
- Subject = Dname polje popunjeno sa podacima korisnika



*Smart card logon sertifikat*



*Ekstenzije za smart card logon*

## Praktična realizacija logovanja putem smart kartica na Windows XP operativne sisteme

Prvi korak praktične realizacije ovog projekta se svodio na skupljanje dokumentacije o proceduri koju Microsoft Windows XP zahteva kako bismo ostvarili cilj. Pored Microsoftovog sajta, na samo još dve lokacije na internetu je pomenut i površno opisan postupak za pripremu logovanja na sisteme preko smart kartica.

Pre početka ovog projekta postavio sam Certification Authority namenjen za potvrdu identiteta fakultetskih web servera i studentskih mailova. Za potrebe autentifikacije i potvrde studentskih mailova otvorio sam novi CA koji je izdao glavni CA i namenjen je samo u tu svrhu. Razvio sam svoj RA mehanizam za zahtevanje i izdavanje sertifikata, i sistem za distribuciju izdatih sertifikata.

Projekat zaštite mail identiteta tj. Digital ID sam realizovao preko OpenSSL programa. U njemu sam generisao samo-potpisan glavni CA, CA za izdavanje DigitalID-a koji je izdat od strane glavnog CA, i njime sam generisao korisničke zahteve, parove ključeva, digitalne sertifikate, pakovao ih u PKCS#12 formatu zajedno sa privatnim ključem i šifrom koja štiti ključ, i slao studentima (sa šifrom za otvaranje).

Prvobitna ideja je bila da iskoristim već napravljenu strukturu PKI sistema. Formiram novi CA koji bi bio potpisan glavnim CA, i njime izdavao sertifikate za logovanje smart karticom.

OpenSSL verzija 0.9.8 – ujedno i poslednja kompajlirana verzija za Windows koju sam mogao skinuti sa interneta, stvarala je mnogo problema oko zahtevanih ekstenzija sertifikata. Nisu sve ekstenzije koje zahteva Microsoft podržane od strane OpenSSL, ali ipak mogu da se ubace po svom broju.

Glavni problem je predstavljalo to što Subject Alternative Name polje, po OpenSSL-u, ne može da sadrži pod polje ili više pod polja. Sertifikati za DC i smart kartice zahtevaju popunjavanje ovog (ovih) polja. Na forumima sam čitao o raznim došetkama koje su ljudi koristili kako bi prevazišli ovaj problem. Potrebne podkolone je trebalo ručno predstaviti u heksa-dekadnom formatu koristeći predefinisani heder i footer ovog polja.

Kako bi za izdavanje korisničkih smart kartica za logovanje ovo bilo pravo mučenje ručno raditi, pokušao sam da pronađem drugo rešenje. Na sajtu OpenSSL-a, pročitao sam da nova verzija 0.9.8b podržava drugačiji način unošenja ekstenzija. Međutim nisam mogao da pronađem kompajliranu verziju, već je na sajtu bio samo izvorni kod. Skinuo sam kod i kompajlirao programom Cygwin. U dokumentaciji sam video kako se sad unose podaci u polje Subject Alternative Name. Isprobao sam i prošlo je bez problema.

OpenSSL-om sam uspeo da generišem sertifikate prema specifikaciji Microsofta. Video sam da zapravo i nije neophodno da se za DC ključevi generišu preko Schannel CSP-a.

Konfiguracioni fajl za ekstenzije u OpenSSL-u bi trebao da izgleda ovako :

```
[ ms_dc ]
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, serverAuth
basicConstraints=CA:FALSE
1.3.6.1.4.1.311.20.2=DER:1e:20:00:44:00:6f:00:6d:00:61:00:69:00:6e:00:43:00:6f:00:6e:00:74:
00:72:00:6f:00:6c:00:6c:00:65:00:72
2.5.29.17=DER:30:32:A0:1F:06:09:2B:06:01:04:01:82:37:19:01:A0:\
12:04:10:AD:C8:0C:83:DC:EC:45:3A:9E:2E:0A:8A:89:8A:EE:76:82:0F:\
70:72:6F:62:61:2E:6D:72:65:7A:61:2E:6E:65:74
crlDistributionPoints = URI:\\proba\crl\dc.crl

[ ms_user ]
basicConstraints=CA:FALSE
crlDistributionPoints = URI:\\proba\crl\dc.crl
keyUsage = digitalSignature
extendedKeyUsage = clientAuth, 1.3.6.1.4.1.311.20.2

# Certificate template "SmartcardUser" (bmp string)
1.3.6.1.4.1.311.20.2=DER:1e:1a:00:53:00:6d:00:61:00:72:00:74:00:63:00:61:00:72:00:64:00:55
:00:73:00:65:00:72
subjectAltName=@altname_sec

[ altname_sec ]
otherName=1.3.6.1.4.1.311.20.2.3;UTF8:k1@mreza.net
```

MS\_DC su ekstenzije za domen kontroler, Subject Alternative Name je napisan u formatu kompatibilnom sa starom verzijom. Polja gde umesto imena promenljive stoji broj su polja koja nisu podržana u OpenSSL-u.

MS\_USER su ekstenzije potrebne za sertifikat za smart card login, Subject Alternative Name je napisan u formatu koji podržava nova verzija.

Za generisanje DC srtifikata koristio sam sledeće komande :

```
openssl genrsa -out dc.key
openssl.exe req -new -key dc.key -out dc.csr -config openssl.txt
openssl.exe x509 -req -days 1825 -in dc.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out
dc.crt -extfile openssl.txt -extensions ms_dc
```

Za generisanje user smart card logon sertifikata sledeće komande :

```
openssl genrsa -out user.key
openssl.exe req -new -key user.key -out user.csr -config openssl.txt
openssl.exe x509 -req -days 1825 -in user.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out
user.crt -extfile openssl.txt -extensions ms_user
```

Za eksport sertifikata i privatnog ključa u PKCS#12 format komandu :

```
openssl.exe pkcs12 -export -in dc.crt -inkey dc.key -out dc.pfx
```

Za generisanje CRL liste CA koristio sam sledeću komandu :

```
openssl ca -genctrl -keyfile CA.key -cert CA.crt -out dc.crl -crl days 1825 -config openssl.txt
```

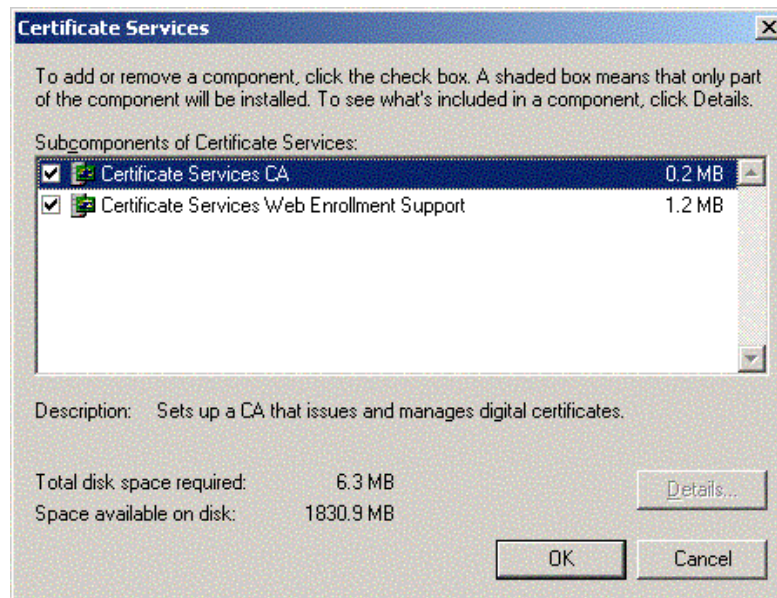
Sa rešavanjem konkretnih tehničkih problema nadao sam se da sam rešio veći deo svojih problema. Međutim, u početku sam zanemario jednu veoma bitnu stvar. Pošao sam od pretpostavke da CRL liste se veoma lako prave i da sa njima neće biti problema. Kao što se vidi iz priložene komande, kreirao sam CRL listu koja će se osvežavati svakih 1825 dana. Tek sam kasnije uvideo koliki je to problem. Čemu zapravo služi CRL lista ako se ona neće redovno updatovati i ako se neće koristiti za ono za šta je namenjena.

Razmišlja sam da razvijem svoj sistem kako bih povezao CRL listu sa korisničkim nalogima na domenu. Ideja mi je bila da periodično vršim proveru korisničkih naloga i ako naiđem na ugašen (disabled) nalog da povučem i sertifikat. Ovo rešenje je zahtevalo dosta sistemskog programiranja kao bi se povezao Microsoft proizvod sa OpenSource proizvodom.

Na forumima sam video da su to i drugi pokušavali i na tome gubili previše vremena. Dosta onih koji su radili na ovome su prešli na Microsoftovo rešenje i ako su to u početku izbegavali.

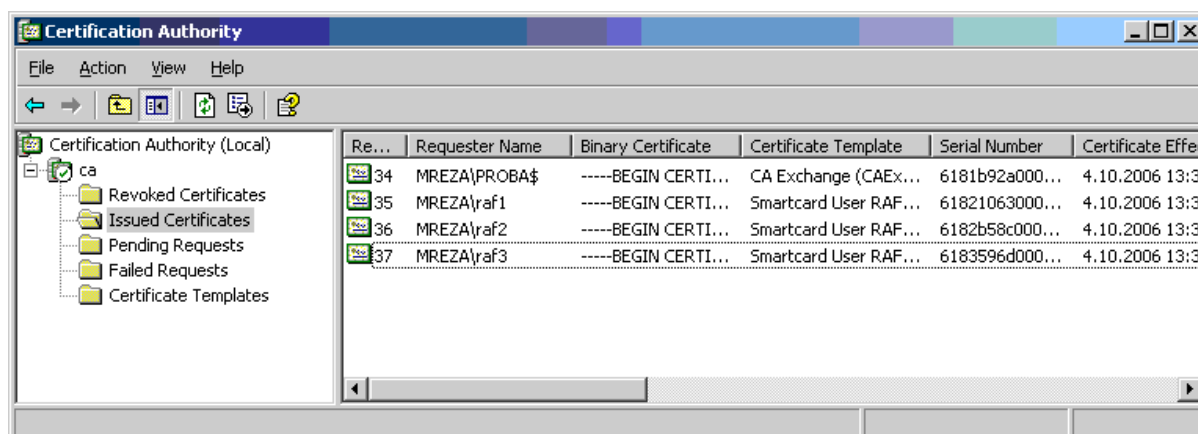
Microsoft Certification Authority je servis koji dolazi uz Microsoft Windows 2003 servere. Njeova namena je da pruži sistem od poverenja i PKI funkcije serverima i korisnicima.

Ono što sigurno izdvaja ovaj servis od svih ostalih je kompletna integracija sa aktivnim direktorijumom. Kada uvidimo da MS CA pruža sve mogućnosti koje su nam potrebne za izdavanje digitalnih sertifikata, upitamo se zašto smo uopšte i pokušavali sa drugim programima, kada nam je ovaj bio „ispred nosa“.



*MS CA servis*

Na početku instalacije MS CA servisa, wizard će nas voditi kroz grupu opcija koje treba popuniti. One se uglavnom odnose na formiranje CA ROOT-a, tj. glavnog, samopotpisanog, CA sertifikata. Popinjavaju se parametri vezani za CRL listu, datum osvežavanja, mesto skladištenja i sl. Microsoft CA zahteva instaliran IIS jer formira virtualni direktorijum i postavlja web mehanizme za kreiranje zahteva i distribuciju sertifikata.



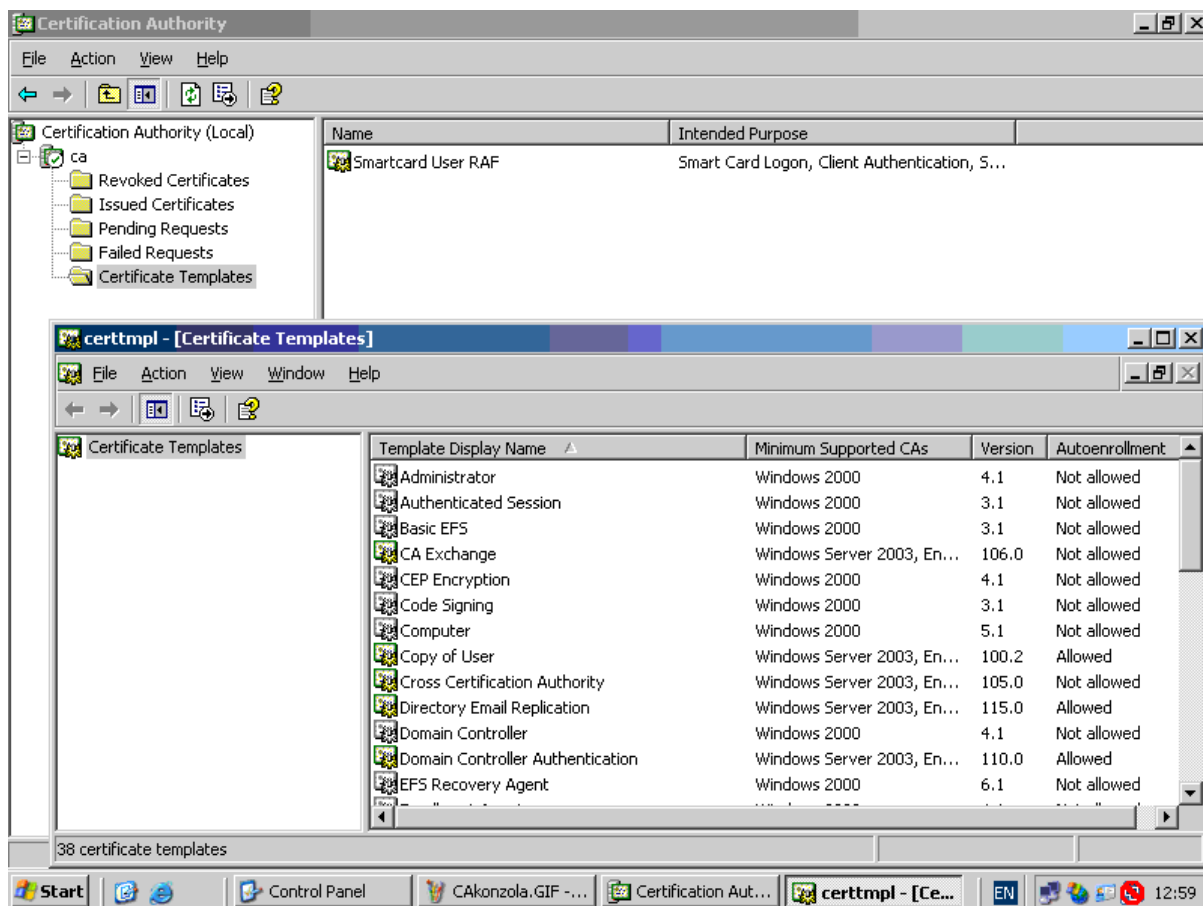
*Konzola MS CA*

Konzola za upravljanje MS CA je u klasičnom Microsoft MMC stilu. Pored opcije za konektovanje na localhost server tu su i opcije :

- Revoked Certificates – spisak svih povučenih sertifikata, sa podacima tima datum povlačenja, razlog povlačenja, kao i kompletni sertifikati u enkodovanom obliku.
- Issued Certificates – spisak svih sertifikata koji su izdati, a nisu povučeni. Ovde se nalaze i podaci koji se mogu videti u sertifikatu, kao i podaci o korisniku koji je zahtevao sertifikat.
- Pending Request – se koristi ako je u CA podešena opcija da se sertifikati ne generišu automatski po zahtevu već je potrebno odobrenje administratora. Ovde se smeštaju zahtevi koji se izdaju nakon odobrenja.
- Failed Request – ako iz bilo kog razloga ne uspe prevođenje iz zahteva u sertifikat ili je zahtev odbijen iz pending polja, zahtevi se pojavljuju u ovom polju kao i obrazloženje nastale greške.

- Certificate Templates – je polje u kome se dozvoljava generisanje sertifikata za određene svrhe.

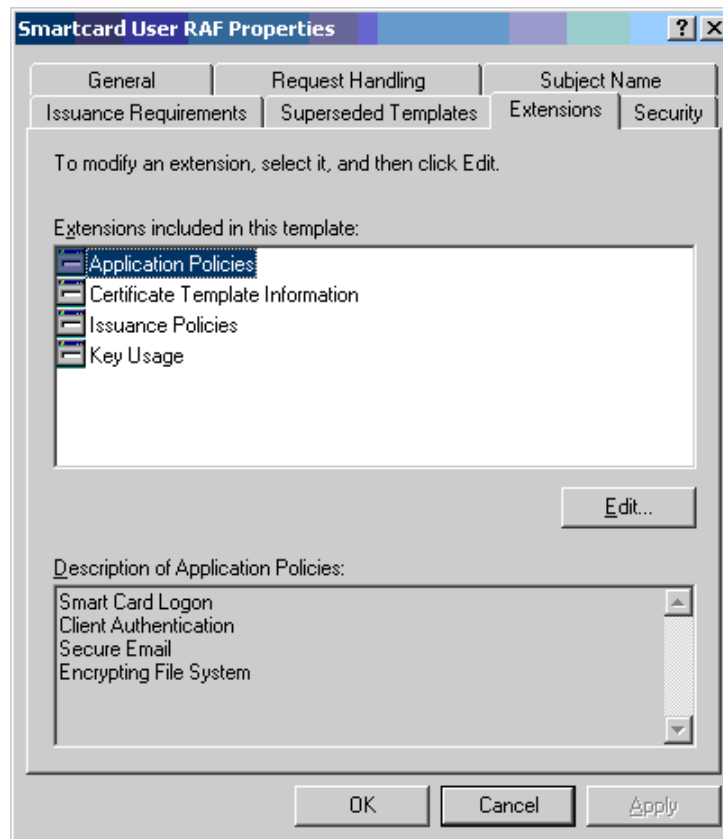
Postoje predefinisane templates – postavke, koje standardno izdaje CA, ali se mogu ubaciti i dodatne kastomizirane.



*Menadžment postavki (templates) sertifikata za izdavanje*

Na prikazanoj slici dozvoljeno je automatsko izdavanje samo sertifikata sa postavkom Smartcard User RAF, dok se u donjem delu slike mogu videti neke predefinisane postavke.

Postavku SmartCard User RAF sam dodatno definisao tako da podržava Smart Card Logon, Email DigitalID, Client Autentification i Encrypting File System za zaštitu fajlova.



*Postavka Smartcard User RAF*

Opremu potrebnu za projekat logovanja na sisteme upotrebom smart kartica čine :

- Čitači smart kartica – svaka radna stanica mora imati čitač smart kartica
- Smart kartice sa PKI funkcijama – svakom korisniku treba izdati smart karticu koja će sadržati par ključeva i digitalni sertifikat.
- CSP – middleware posrednik između sistema i kartice

Čitači smart kartica se teško nalaze jer malo ko ih kupuje, ali ipak može da se nabavi u slobodnoj prodaji.

Sa Smart karicama stvar je dosta komplikovanija. Firme koji uvoze smart kartice uglavnom prodaju bankama ili većim firmama koje su prethodno kupile neke njihov proizvod. Duže vreme sam komunicirao sa više firmi koje prodaju smart kartice, tražeći od njih da mi izdaju ili prodaju do 10 kartica zbog ovog projekta. Uglavnom su odbijali da pomognu uz izgovor da ne mogu da prodaju tako malu količinu nepoznatom licu, jer se plaše da može doći do zloupotrebe bankarskih kartica.

Kontakt sam ostvario i sa firmom NetSet, gde sam pozvan na razgovor. Saslušali su me i predložili da ostvare konkretniju saradnju sa fakultetom. Fakultet je takođe bio zainteresovan za saradnju što je proizišlo sporazumom o saradnji. Nakon ovog sporazuma uspeali smo da iznajmimo 3 čitača smart kartica i 3 kartice. Firma NetSet nam je izašla u susret i izdala i CSP koji je njihovo komercijalno softversko rešenje. Iz ovih razloga mogu reći da, zahvaljujući firmi NetSet iz Beograda, ovaj projekat ima i praktičnu vrednost.

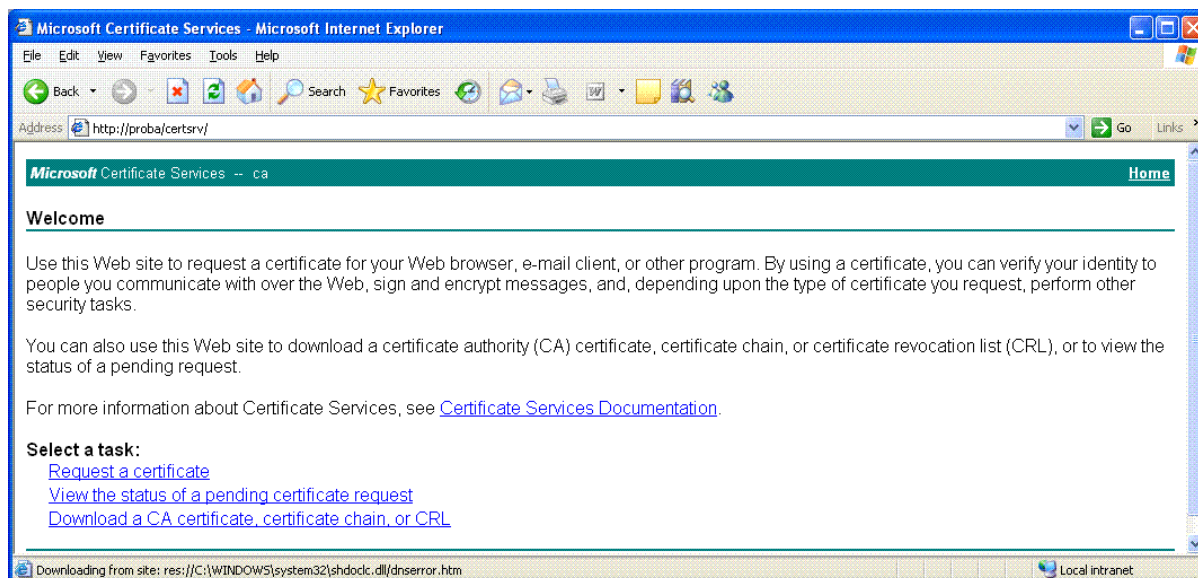


*Smart kartice firme NetSet*



*Čítač smart kartica*

Proces izdavanja sertifikata kod Microsoft CA je dosta pojednostavljen. Svodi se na popunjavanje formulara na web portalu MS CA. Do web protala se dolazi preko sajta <http://<caserver>/certsrv/> gde je <caserver> ime računara gde je instaliran MS CA, u našem slučaju proba.



*Certsrv web portal MS CA*

Prilikom ulaska u web portal, upitani smo za autentifikacione podatke, korisničko ime i šifru. Na portal se može ulogovati bilo koji korisnik domena.

Opcije početnog ekrana su :

- Request a certificate – zahtev za sertifikatom
- View the status of a pending certificate request – ako ste poslali zahtev za sertifikat, i još se čeka na njegovo odobrenje, ovde možete videti status vašeg zahteva.
- Download a CA certificate, certificate chain, or CRL – pruža linkove prema ROOT CA sertifikatu, CRL listi CA, i lancu sertifikata ukoliko postoji CA iz više nivoa.

Microsoft je predvideo mogućnost da Administrator generiše sertifikate za sve korisnike i pripremi im smart kartice. Međutim, NetSet-ov CSP podržava postavljanje ključeva isključivo u već kreiran kontejner (direktorijum), ali ne i da sami kreiramo, što MS CA zahteva za ovu uslugu.

Posledica ovoga je to što svaki korisnik mora da se uloguje da bi mu kreirali sertifikat.

Kada se korisnik uloguje treba da izabere opcije sledećim redom :

- Request a certificate
- Create and submit a request to this CA.
- Use existing key set
- U polje Container Name treba uneti \\.\
- Submit
- Treba dozvoliti Internet Exploreru da pristupi čitaču
- Uneti PIN smart kartice

Ako u kontejneru ne postoji generisan par ključeva, CSP poziva funkciju za generisanje ključeva na kartici. Ako postoji, formira se zahtev na osnovu podataka iz aktivnog direktorijuma i javnog ključa sa kartice i prosleđuje CA. Ako je CA tako

podešen, odmah nakon zahteva dobijate poruku da je sertifikat kreiran i nudi vam se mogućnost upload-a na karticu. Sve što treba da uradite je da kliknete na link Download certificate on the smart card i CSP će obaviti ostalo.

Nakon punjenja kartice ključevima i sertifikatom, obavezno promeniti inicijalni PIN i PUK kod. Promena se može izvršiti preko Token Manager-a koji dolazi uz NetSet-ov CSP.

Nezgodono jeste to što moramo pozvati svakog korisnika da se uloguje u web portal da bi mu kreirali karticu, ali i sa tim ovo je veoma brz način da se uvede logovanje preko smart kartica.

U MS CA konzoli sertifikati se mogu, pod opcijom Issued certificate, povući i obrazložiti razlog povlačenja. Sertifikati sa razlogom Holded certifcate, se posle mogu vratiti, dok sa drugim razlozima sertifikat se mora ponovo izdati. CRL treba podesiti da se što češće osvežava, jer Windows workstation SmartCard proces proverava CRL listu samo ako misli da je izdata nova verzija, u suprotnom kešira CRL do njenog novog izdavanja.

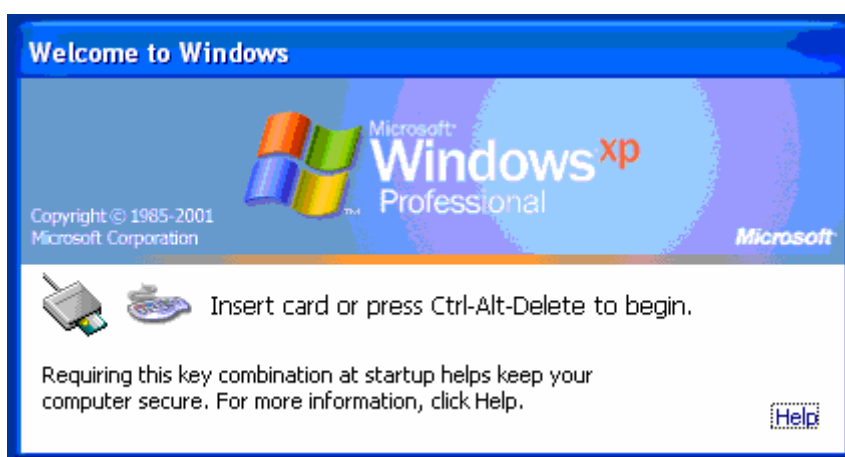
## Zaključak

Cilj ovog projekta je bio da se unapredi sigurnost poboljšanjem načina autentifikacije korisnika prilikom logovanja na Windows XP operative sisteme.

Na svaku radnu stanicu treba uraditi sledeće :

- Priključiti čitač smart kartica
- Instalirati drajver za čitač smart kartica
- Instalirati NetSet-ov CSP

Promena prilikom logovanja izgleda ovako :



*Ekran za logovanje nakon instalacije čitača smart kartica.*

A nakon ubacivanja kartice potrebna je verifikacija PIN koda :



*Verifikacija PIN koda nakon ubacivanja kartice u čitač*

Koliko je ovaj sistem autentifikacije siguran govori činjenica da je hardverski modul, tj. smart karticu je nemoguće kopirati, jer privatni ključ nikada ne napušta karticu. U slučaju prodora u elektroniku kartice, štićeni podaci se uništavaju.

Za slučajeve krađe ili nestanka kartice, korisnik mora što pre da obavesti administratora, kako bi se sertifikat sa te kartice našao na CRL listi.

PIN kod služi samo kao još jedan stepen zaštite tako da iako neko ukrade karticu ne može, bez znanja PIN koda, zloupotrebiti vaš identitet. Na karticama koje smo dobili od NetSet-a, dozvoljeno je samo 3 puta da se pogreši PIN, nakon čega se kartica blokira.

Kartica se može deblokirati poznavanjem PUK koda, koji zna samo administrator. Ako se i PUK kod pogrešno unese 3 puta, kartica se trajno zaključava i ne može se više zloupotrebiti.

Proširivanjem ekstenzija digitalnog sertifikata postigli smo i sledeće :

- Digital ID – pruža mogućnost korisnicima da, uz pomoć iste smart kartice, dokažu identitet, integritet, i sačuvaju tajnost svoje elektronske pošte. Potrebno je samo krostiti mail client koji podržava S/MIME, kao npr. Outlook Express
- Klijentska autentifikacija – pruža mogućnost autentifikacije korisnika bez korišćenja korisničkog imena i šifre. Podrška ovoj autentifikaciji zavisi od aplikacija. Može se koristiti za autentifikaciju na Web-u uz odgovarajući ActiveX script.
- File encryption system – MS Windows podržava enkripciju na NTFS particijama. Može se primeniti na fajl, folder ili celu particiju. Ovim putem napravićete vaše fajlove dostupne samo uz smart karticu.

Uz sve ove mogućnosti koje pruža upotreba PKI i smart kartica, mislim da je lako doneti odluku za investiranje u hardver i softver koji čine ovaj sistem.

## Literatura

- Bezbednost računarskih mreža (2006)  
Doc. Dr. Milan Marković dipl. inž. [milan.markovic@bankaintesa.co.yu](mailto:milan.markovic@bankaintesa.co.yu)  
Mr. Goran Đorđević dipl. inž.
- Guidelines for enabling smart card logon  
Microsoft ([www.microsoft.com](http://www.microsoft.com)) Article ID:281245  
<http://support.microsoft.com/kb/281245/>
- How to import third-party certification authority (CA) certificates into the Enterprise NTAAuth store  
Microsoft ([www.microsoft.com](http://www.microsoft.com)) Article ID: 295663  
<http://support.microsoft.com/kb/295663/>
- Requirements for Domain Controller Certificates from a Third-Party CA  
Microsoft ([www.microsoft.com](http://www.microsoft.com)) Article ID: 291010  
<http://support.microsoft.com/kb/291010/>
- OpenCA ([www.openca.org](http://www.openca.org))  
Poglavlje 3. Microsoft  
Chapter 7. Client Support
- OpenSSL ([www.openssl.org](http://www.openssl.org))
- Cygwin ([www.cygwin.com](http://www.cygwin.com))
- NetSet ([www.netset.co.yu](http://www.netset.co.yu))